HACKER JOURNAL

Come si rubano le IMPRONTE DIGITALI



FLASH
REALIZZIAMO *UN MOTORE* DI RICERCA

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CIFRARIO PERFETTO

I SEGRETI DELLA VOCE VIA INTERNET

QUATTORDICINALE ANNO 3
15 LUGLIO 2004 - 29 LUGLIO 2004
SPED. IN ABB. POST. 70% - MILANO

4ever

Anno 3 – N. 55
15 Luglio 2004 - 29 Luglio 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

HACKER JOURNAL

editoriale

I compiti delle vacanze

Non so voi, ma si sente aria di vacanza perfino in rete. Ed è vero. Guardi i blog della gente e c'è già chi scrive da lontano, o racconta del condizionatore, o smette di scrivere e se ne va in piscina o dove altro. Voi che fate? Avete voglia di raccontare a questa accaldata redazione che cosa si combina in ognuno delle decine di migliaia di nodi umani e superumani che compongono questa fantastica rete di coltivatori della conoscenza chiamata Hacker Journal? Leggeremo volentieri quello che arriva e se arriva qualcosa di divertente e interessante lo pubblicheremo pure.
Tornando in argomento-estate, i mesi caldi sono quelli più proficui per un hacker. Il perché è chiaro: le scuole chiudono e si può studiare anche qualcosa di diverso dalla storia degli Assiro-babilonesi, poco interessante a parte il fatto che contavano in base dodici (come si scrive 2004 in base dodici?). Le aziende restano aperte, ma i ritmi si rilassano e si può dare un'occhiata in più a un manuale interessante o a un forum con le dritte giuste.
Anche i genitori sono più tranquilli, o più colpiti dal caldo, e se la prendono meno – o proprio non ce la fanno – se si sta al computer a scoprire qualcosa di nuovo o a collaudare un programmino appena scritto.
L'estate è anche la stagione d'oro per l'ingegneria sociale. I centralini sono più distratti, le segretarie non ci badano, i bidelli lasciano passare tutto, se c'è da strappare un permesso proibito o guardare dove non si potrebbe è il momento più adatto per provarci.



Purtroppo ne approfittano anche i disonesti. Quelli che si mettono in fila alle casse della pizzeria per sbirciare le carte di credito altrui, o controllano i lucchetti delle biciclette alla ricerca di quello chiuso male. Ma non sono hacker, lo sappiamo già: sono solo stronzetti e vediamo di non dargli spazio, né facilitargli il compito.
Noi hacker, come potremmo passare l'estate? Il primo suggerimento, ma era ovvio: leggiamo Hacker Journal anche in spiaggia, o sui monti. Il secondo, meno ovvio: conosciamo gente. Parliamo con il vicino di ombrellone, con la signora Gina della Pensione Gina, con quella della classe di fianco che non c'è mai stata occasione di scambiare due chiacchiere. Per un hacker il rapporto umano è uno dei tesori più importanti che ci siano.
E infine i compiti delle vacanze, no, il compito delle vacanze: prendersi un'ora, o un giorno, o una settimana, e programmare. Anche una cosa piccola, anche una sciocchezza, anche scrivere Hello world in Javascript e abbandonarsi sfiniti alla soddisfazione, con in mano una granita ghiacciata.

Buone vacanze a tutti!
theGuilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea: Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Contents by MDR

Service: Cometa s.a.s.

DTP: Romina "Nikita" Grasselli, Cesare "Clark" Salgaro, Cristina "Caffeina" Morelli, Veronica "Pollon" D'Adda, Ivan "Insomnia" Roman, Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

freeHACKnet

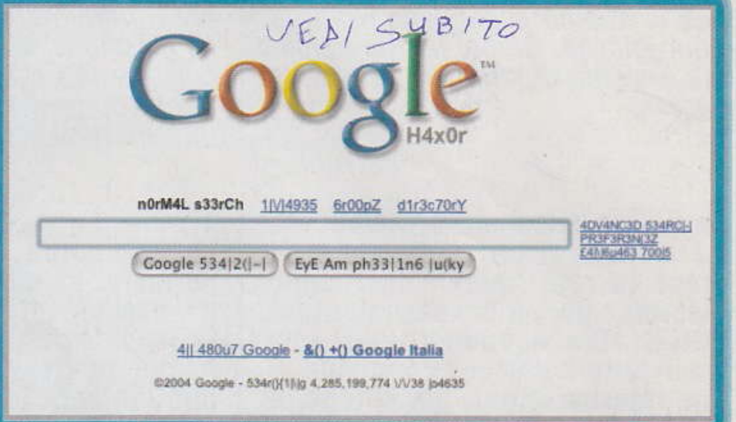
UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

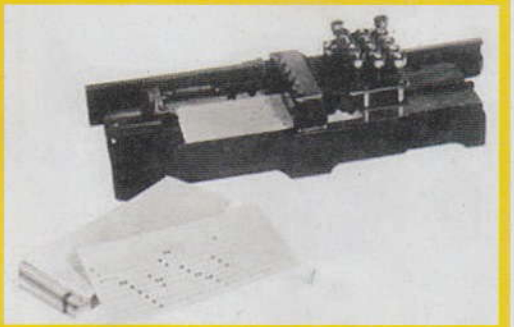
NEWBIE   MID HACKING   HARD HACKING

Google, anzi, G00g|3

Il motore di ricerca più famoso al mondo ha pensato anche alla comunità hacker…

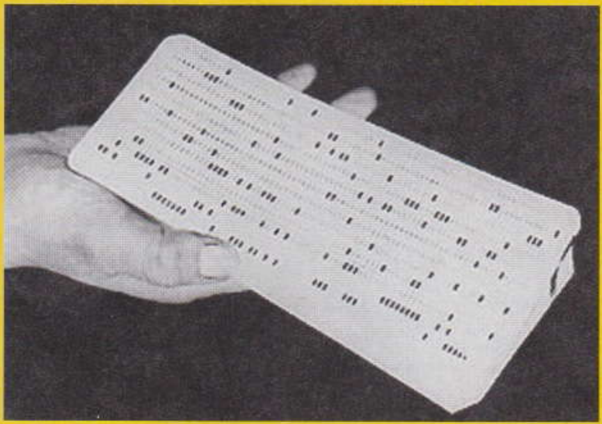


I BEI TEMPI ANDATI



…ricordo quando ho punzonato una bella quantità di schede perforate di codice sorgente su una punzonatrice IBM 010. Dodici chiavi dati, una per riga. Più una chiave per scavalcare l'avanzamento automatico delle colonne e una chiave spazio per saltare una colonna oppure per farla avanzare se uno si dimenticava di rilasciare la chiave di blocco prima dell'ultima riga del carattere.

Ah… per un po' di tempo la 010 rimase disponibile anche con l'avvento della 024 e della 026, con le loro comode tastiere e funzioni di programmazione. Ma erano poche e si faceva la coda. In certi momenti era più veloce punzonare una ventina di schede perforate sulla 010 che aspettare una macchina libera.



John

Self-made Website

Ciao! Vorrei segnalare il mio sito! Io ho 14 anni e me lo sono fatto tutto da solo e speravo che voi riusciste a segnalarlo nel prossimo numero! Leggo sempre i vostri articoli! Siete grandi! My site: http://www.wba.it/Marri%20dj%20site%20folder/Index.htm.

Michele (Marridj)

Nuova Password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troveremo arretrati, sfondi, informazioni e approfondimenti interessanti. Con alcuni browser, può capitare di dover inserire due volte gli stessi codici. Non fermiamoci al primo tentativo!

USER: euro

PASS: 269W

SERVER OF FORTUNE

Mi diverto a giocare a Soldier of Fortune 2 in rete. Vi scrivo per una cortesia. Il mio clan è appena nato e quindi avremo bisogno di un server sempre più grande perché ci stiamo espandendo giorno dopo giorno. Quindi la mia richiesta è quella di farci voi un grande server.

darkshine

La nostra missione è pubblicare HJ e non alzare server per il gioco in rete (quanti dovremmo alzarne, poi, per accontentare tutti?). Ma scommettiamo che tra i lettori c'è chi condivide il tuo interesse per SoF2 (che è molto bello) e ha anche un server da mettere a disposizione. Ci scriva e inoltreremo la mail a darkshine!



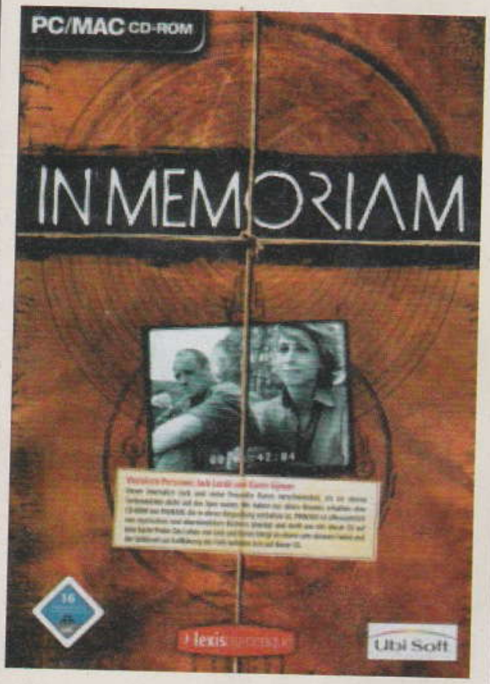
▲ Chi ha un server per ospitare darkshine e il suo clan di soldati di fortuna?

IN MEMORIAM PRIVACY

Ultimamente ho acquistato un gioco della Ubisoft che si chiama In Memoriam. Con mia grande sorpresa ho scoperto che questo gioco mi fa ricevere delle vere e-mail da internet e dalle segnalazioni di Zone Alarm ho notato che il programma sfrutta parecchio la connessione a Internet! Ora mi chiedo: non c'è pericolo che questo gioco trasmetta a mia insaputa informazioni private?

Il Corvo

Vai tranquillo, non corri nessun pericolo. La casa produttrice non ha nessun interesse a rovinarsi la reputazione per un gioco. Anche se riceve tuoi dati, come minimo sarà assai attenta a non abusarne.



▲ Per aumentare il realismo del gioco, una volta installato, iniziano ad arrivare mail misteriose e inaspettate ma non c'è da preoccuparsi. Al limite c'è da chiedersi dove possono arrivare questo tipo di giochi. Qualcuno busserà presto alla nostra porta?



OPINIONE SULL'HACKING

Entrare in un computer a titolo di "studio" è un atto da hacker? La nostra intera comunità si divide a questa domanda. La mia (modesta) opinione, è riassunta, molto semplicemente, nel seguente esempio.
Cammini per strada, guardi le case che ci sono e ne trovi una che sembra avere la porta aperta. Cosa fai? Suoni il campanello e avverti, oppure attraversi il giardino, controlli che la porta sia effettivamente aperta, entri (magari leggi la posta, già che ci sei, per curiosità, mica per far danni...) poi cerchi il padrone di casa, gli picchietti una spalla e gli dici "Ehi, hai la porta di casa aperta..."

Alt[O]s

Ovviamente non c'è hacking serio e condivisibile senza rispetto per gli altri (e per i loro dati). Ma se la questione fosse sempre così netta non ci sarebbe bisogno di dibattere. Pensiamo a Kevin Mitnick, per esempio. Non c'è dubbio che la sua applicazione disinvolta dell'ingegneria sociale lo abbia portato a oltrepassare i limiti (e ha pagato per questo). Ma come valutare effettivamente la sicurezza interna di un sistema senza penetrarvi?

GUAI A CHI TOCCA WINDOWS

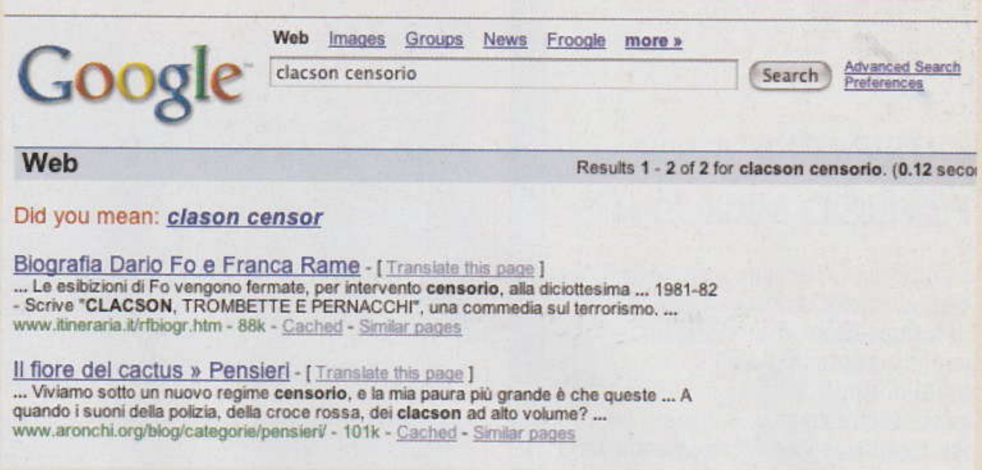
Stavo gironzolando nella vostra chat, visto che avevo un problemino con XP per vedere se qualche vero hacker mi avrebbe aiutato, ma mi sono accorto di una cosa: ci sono tanti fanatici di Linux (anche se non posso dargli torto) che odiano Windows, ma non sanno quasi neanche come funziona. Ora mi dico: non usate Windows, va bene, è più stabile Linux, va bene, ma cosa criticate Windows XP se non siete riusciti nemmeno ad aiutarmi a risolvere un problemino con l'hard disk. XP non sarà stabile come Linux, avrà i suoi problemi, Linux sicuramente avrà tanti pregi, ma se non conoscete bene il nemico almeno statevene zitti e non criticatelo!

NOTTURNO

Non esistono nemici, esistono solo scelte. Noi tifiamo Linux ma rispettiamo chi tifa Windows e chi sa giudicare i pregi e i difetti del proprio sistema con obiettività e serenità. E se veramente è impossibile mettersi d'accordo, beh, perché non sfidarsi a Battle for Wesnoth?

▼ Battle for Wesnoth, un fantasy game a turni, semplice ma avvincente, con gioco in rete locale e via Internet. Funziona praticamente su tutti i sistemi operativi conosciuti ed è un sistema eccellente per risolvere le dispute facendo amicizia, a http://www.wesnoth.org.





▲ Cercare due parole italiane su Google e trovare un solo sito in risposta: ecco un googlewhack. Il clacson censorio è scaduto (i siti sono due). Chi è capace di trovare altri googlewhack?

C'È SEMPRE UN GOOGLEWHACK DA QUALCHE PARTE

Credo di aver trovato un altro googlewhack digitando clacson censorio.

Baudelaire

Non è durato nel tempo, ma complimenti lo stesso!

TRUCCARE IL REGISTRO

Ho 15 anni e vorrei sapere qualche trucco per il registro di windows 2000. Del tipo come rendere invisibile il pannello di controllo o alcuni codici da inserire per modificare qualche programma.

Lorenzo Maddaluno

Ogni tanto questo tema ritorna su Hacker Journal, quindi continua a seguirci. Nel frattempo, degli innumerevoli posti su Internet dove puoi trovare notizie a riguardo, ti segnaliamo http://windows.about.com/cs/registrytips/. Se trovi qualcosa che ti piace faccelo sapere!

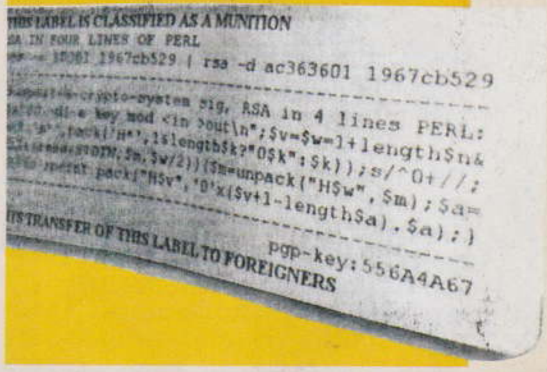
COMPILANDO PERL

Ciao, sono un Newbie con la N maiuscola, e detto questo passo alla domanda: programmo in Perl da qualche settimana (su Windows XP) e volevo sapere se esiste qualcosa che trasforma i miei script in file eseguibili. L'editor che uso (Dzsoft Perl Editor) mi consente di eseguirli da prompt dei comandi ma io voglio vedere il mio .exe. Sapreste indicarmi un software free che lo faccia?

N4zguL

Da Perl 5.005 in poi il linguaggio comprende un modulo, B, che permette di creare eseguibili binari. Trovi approfondimenti, per esempio, a http://www.perldoc.com/perl5.6/lib/B/Bytecode.html o http://www.dwam.net/docs/perl/lib/B.html.

▼ RSA in quattro righe di Perl



HOT!

ITRIP MINI PER IPOD MINI



Tutto mini, ma non nelle prestazioni. Il trasmettitore iTrip si infila sopra l'iPod mini di Apple e trasmette sull'autoradio, su frequenze inutilizzate, i brani MP3 registrati nell'iPod di Apple.
Che in Italia ci siano però frequenze inutilizzate sulla banda FM è cosa che sconcerta. Vale una verifica...

TISCALI STRANGOLA IL P2P

Chi ha Tiscali satellitare e scarica "troppo" si vedrà ridotta la banda. Gli utenti di Tiscali Sat Premium che scaricano più di 1,5 GB nel mese passeranno da 400/128 kbps a 128/24 kbps, mentre chi ha acquistato Tiscali Sat Lan potrà scaricare tre gigabyte nel mese prima di vedersi ridotta la connessione.
Secondo Tiscali la decisione è stata presa per disincentivare gli usi della connessione, come FTP e P2P, definiti "anomali".
Noi troviamo anomalo che un provider ficchi il naso nelle faccende degli utenti. Se uno consuma banda, che la paghi. Ma se la paga, ha diritto di consumarla fino a quando non viola la legge.



Fai un abbonamento costoso a Tiscali satellitare e loro ti riducono la banda se ne consumi troppa. Sputano nel... piatto dove mangiano.

GIF LIBERATION DAY!

18 giugno 2004, l'Europa è libera! Di fare che? Ma naturalmente di utilizzare tutte le immagini GIF che vuole senza dover pagare nulla a nessuno. Perché non era già così? No.
GIF (Graphics Interchange Format) è un formato per immagini usato dal 1987 da CompuServe al posto del precedente formato RLE che era solo in bianco e nero. GIF utilizza la compressione LZW, molto più efficiente di RLE adottato da altri formati immagine come PCX e MacPaint.
Ma... l'algoritmo di compressione LZW sul quale è basato il formato GIF, è un brevetto di CompuServe e Unisys. Prima del 1994, le società in questione non pretesero il pagamento di nulla, ma dal 1995 decisero di iniziare a chiedere il pagamento dei diritti di utilizzo del brevetto, per qualunque programma commerciale capace di creare file in formato GIF. L'utilizzo di immagini in formato GIF era così diffuso che alle aziende non rimase che pagare. Tra parentesi: fu così, anche, che nacque PNG, un formato senza restrizioni legali. Ma oggi è il tempo del riscatto. Già dal 20 Giugno 2003 nessuna azienda americana deve più pagare CompuServe e Unisys per la creazione di GIF e dal 18 giugno di quest'anno nemmeno noi. In Giappone e Canada dovranno aspettare circa una settimana: le scadenze sono rispettivamente il 20 Giugno e il 7 Luglio 2004. E pensare che anche IBM aveva un brevetto su questo algoritmo, ma non si è mai sognata di chiedere nulla a nessuno!

UNISYS Imagine it. Done.

MAI PIÙ FILI AL MONITOR!



Three-Five Systems ha eliminato in un botto tutti i fili che vanno ad attaccarsi al monitor, tranne l'alimentazione. Il monitor wireless è un 1024x768 a 30 frames per secondo, utilizza Wi-Fi 802.11a, quindi ad altissima velocità e finalmente ci consente di tenere il monitor sulle ginocchia mentre la CPU è lontana fino a una trentina di metri. Ovviamente la stessa società ha introdotto il set completo: tastiera, mouse e monitor wireless fanno diventare portatile, perlomeno in ambito casalingo o d'ufficio, anche il computer più grosso e potente. Dalla parte del case della CPU si collega un trasmettitore/ricevitore alle normali prese VGA, tastiera e mouse. Fa tutto da solo, è compatibile con i sistemi operativi attuali e plug-and-play. Affascinante, ma se abbiamo tutte queste voglie di mobilità non vale la pena prendersi un portatile?

JAVA FA UN PASSO VERSO L'OPEN SOURCE

Sun Microsystems ha annunciato di recente la disponibilità su java.net del codice sorgente relativo alle interfacce di programmazione del linguaggio Java 3D.
Non è ancora l'apertura integrale del codice di Java, ma costituisce sicuramente un grande passo avanti, che può solo giovare alla causa del linguaggio di Sun e a quella più generale del software libero.



Java 3D serve anche per realizzare meraviglie nella genetica.

CUCCA IL WIFI COL PORTACHIAVI

Andare in giro con il portatile e individuare segnali WiFi a cui agganciarsi non è più così difficile (se mai lo è stato). È sufficiente attaccare le chiavi di casa o dell'automobile a WiFi Seeker, un portachiavi che costa circa trenta dollari. Lo si compra su http://www.wifiseeker.com/ e becca tutti gli hot spot che lavorano sui 2,4 GHz, la frequenza dello standard 802.11. Un pulsante e una serie di led: se si accendono siamo in presenza di segnale WiFi. È ora di collegarsi.



FU VERO NETSTRIKE?

È passato il blocco del sito del Ministero dei beni culturali, altrimenti noto come Netstrike contro il decreto Urbani, ma le polemiche restano. Da una parte quelli che ritengono l'iniziativa un successo, destinato a spingere il Ministero a modificare in modo più liberale il decreto; dall'altra varie comunità (per esempio Ziobudda.net) dove vari commentatori, pur condannando il pessimo impianto del decreto, criticano fortemente la scelta di ostruire l'accesso a un sito realizzato con denaro pubblico e che in fin dei conti è al servizio di tutti, compresi quelli che lo vogliono navigare decreto o non decreto. Tanto più che l'iniziativa del netstrike è partita da un comitato apparentemente più interessato alla lotta contro l'avversario politico che all'effettiva libertà di comunicazione e scambio in Rete. Boicottare i boicottatori?



Atto rivoluzionario contro i nemici dell'informazione che si annidano nelle istituzioni oppure gesto anacronistico lesivo delle libertà generali? La polemica sul netstrike continuerà.

FINALMENTE SQUADRE CHE CORRONO

Mentre scriviamo si è aperta l'edizione 2004 della RoboCup, il campionato mondiale del calcio giocato da robot, che si è svolta contemporaneamente alle finali degli Europei di calcio (umano). Il nome dei vincitori robotici lo si può vedere su http://www.robocup2004.pt/. Lo spettacolo per ora latita, in attesa di riuscire a fronteggiare una squadra di umani per l'anno 2050, ma garantiamo l'assenza di sputi e la possibilità di trovare giocatori fusi, ma non dalla fatica e dal doping.



Lo vediamo male nel gioco aereo e non ha neanche i piedi. Ma i suoi nipoti sfideranno quelli di Totti nel 2050.

HOT!

ANDARE IN BIANCO ORA È UN'OCCASIONE

Dal 9 luglio e fino all'11 aprile 2005 è aperto il concorso indetto da Seat-Pagine Gialle per trovare giovani artisti italiani tra i 20 e i 35 anni a cui affidare le copertine degli elenchi telefonici dell'anno prossimo. La pagina dedicata al concorso si trova all'indirizzo http://www.paginebianchedautore.it/. Con tutta la creatività che dimostrano i lettori di Hacker Journal, scommettiamo che vincerà uno di noi?



INFETTI NAVIGANDO SU SITI SICURI

L'americano CERT, Computer Emergency Readiness Center, ha lanciato l'allarme per un tipo particolare di attacco che sta venendo portato su Internet. I pirati, stavolta, penetrano nel server del sito bersaglio e modificano alcune pagine inserendo uno script malevolo di nome JS.Scob. Quando un navigatore apre le pagine infettate scarica il codice e rischia grosso, pur non accorgendosi di nulla.



Indovina indovinello, i siti colpiti risiedono tutti su server che usano software Microsoft IIS 5 e l'attacco riesce solo se la vittima visita il sito con Internet Explorer 6. Tanto per cambiare. Un consiglio, no, due: server Apache e browser Mozilla. Si vive meglio.

Dietro la carta di credito

Come funziona il codice di una carta di credito è una sciocchezza tale che si fatica a crederlo. Ma come è fatta una carta magnetica e che dati contiene, e ancora, che standard utilizza?

Il codice di una carta di credito, come spiegato in un numero precedente di HJ, deve verificare essenzialmente la somma delle cifre pari sottratta alla somma delle cifre dispari dando come risultato zero oppure dieci oppure un multiplo di dieci.
È più interessante scoprire che cosa è scritto invece nella banda magnetica delle carte e, di conseguenza, che tipo di dati ci portiamo nel portafoglio senza saperlo.





▲ *Ingrandimento vertiginoso della superficie magnetizzata di una banda.*

Standard fisici

Dimensioni, forma e altre caratteristiche fisiche delle carte di credito sono governate dallo standard ANSI X4.13, American National Standard for Financial Services - Financial Transaction Cards. Lo standard interessa soprattutto gli ingegneri (e gli hacker!) e definisce posizione e dimensioni di banda magnetica, spazio per la firma e scritte in rilievo. Vengono definiti anche la formula di Luhn (usata per determinare il numero della carta) e aiuta a definire il



▲ *Le bande magnetiche delle tessere sono fatte più o meno tutte allo stesso modo, da un comune badge a una carta di credito.*



LA PRIMA TRACCIA

Codifica: 210 bit per pollice
Tipo di codifica: sei bit per un set di 64 caratteri alfanumerici più alcuni caratteri speciali.
Capacità: 79 caratteri, sei dei quali sono caratteri di controllo riservati.
Dati contenuti: numero della carta, codice nazione, nome del titolare, data di scadenza e "dati discrezionali" (a scelta della società emittente).

LA SECONDA TRACCIA

Codifica: 75 bit per pollice
Tipo di codifica: quattro bit per i numeri da 0 a 9, più tre caratteri delimitatori, due caratteri di device control e uno inutilizzato.
Capacità: 40 caratteri, compreso un Longitudinal Redundancy Check (LRC) a limitazione degli errori di lettura.
Dati contenuti: numero della carta, codice nazione (opzionale), data di scadenza e "dati discrezionali".

LA TERZA TRACCIA

Codifica: Come la prima traccia.
Tipo di codifica: Come la prima traccia.
Capacità: 107 caratteri.
Dati contenuti: Praticamente non viene più utilizzata, per ragioni di sicurezza.

tipo di carta in funzione di come è composto il numero.
Ci sono tre insiemi di caratteri utilizzabili sulle carte di credito: OCR-A, così come è definito nello standard ANSI X3.17; OCR-B secondo la definizione ANSI X3.49 e Farrington 7B, in accordo alle specifiche dello stesso ANSI X4.13. Il nome OCR deriva dal fatto che sono fatti per essere letti agevolmente in automatico dal computer, via Optical Character Recognition (Riconoscimento ottico dei caratteri, per l'appunto).

Standard di codifica

Lo standard ANSI X4.16 (American National Standard for Financial Services - Financial Transaction Cards - Magnetic Strip Encoding) definisce le caratteristiche fisiche, chimiche e magnetiche delle tre tracce di codifica previste. Alcune carte possiedono anche una quarta traccia. Questo vale per tutte le carte con banda magnetica e non solo per quelle di credito. Nei riquadri possiamo leggere come sono composte le 3 tracce standard della banda magnetica. In un prossimo articolo affronteremo il tema della frode con le carte di credito: quali sono i tipi più comuni e qualche consiglio per difendersi.

Reed Wright
reedwright@mail.inet.it

NO PROFIT DA NON CREDERE



▲*No profit corporation! Incredibile, ma vero.*

Scoprirlo è uno shock per molti, ma è vero. La VISA (o MasterCard, se è per quello) è una corporation no profit. Sembra un'assurdità ma è quasi ovvio, considerando che VISA in quanto tale non emette carte di credito, emesse in realtà dalle banche che appartengono al circuito. VISA è sostanzialmente una coalizione di banche sotto il cui nome viene svolta attività comune di marketing e di collaborazione. VISA non pone condizioni particolari alle banche che ne fanno parte e tutto il flusso di denaro viene amministrato e approvato direttamente dalle banche componenti. Molte banche piccole che fanno parte del gruppo si appoggiano a banche più grandi o al limite a VISA per la gestione del database delle proprie carte o per l'approvazione delle transazioni, ma questo è tutto. Bizzarro, vero?

E-COMMERCE

Il sistema di verifica delle carte di credito viene utilizzato dai siti Web di e-commerce. Viene infatti controllata la corrispondenza dei numeri prima di inviare la richiesta allla banca.

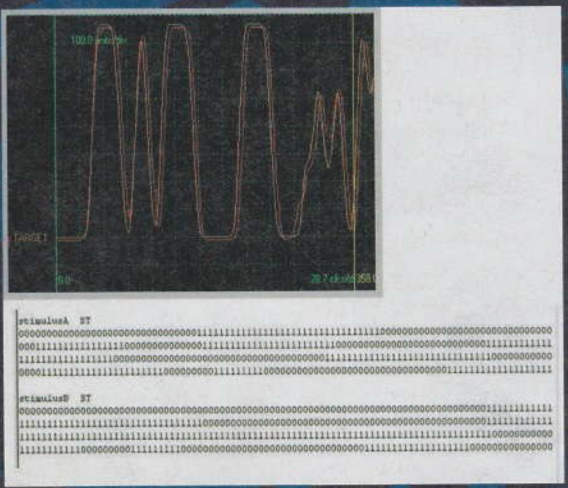




ONE-TIME PAD:

Questo cifrario, in teoria, è inviolabile. Se la chiave viaggia sicura

Un one-time pad (letteralmente, taccuino usa-e-getta) è in principio un cifrario simmetrico completamente inviolabile. Simmetrico significa che usa la stessa chiave per la cifratura e la decodifica. Per tutti i cifrari simmetrici esiste un problema di riuscire a scambiare la chiave di cifratura tra mittente e destinatario, altrimenti quest'ultimo non potrà decodificare il messaggio. Ma se la chiave riesce a essere scambiata in modo sicuro, il cifrario è inviolabile anche in pratica.



In molti laboratori lo XOR, cuore dei cifrari one-time pad, costituisce un'operazione eseguitissima.

La chiave di cifratura migliore per un cifrario one-time pad è una sequenza di bit il più casuale possibile. Generare numeri casuali (random) non è una sciocchezza ed è meglio avere un buon generatore a disposizione, sia esso un algoritmo che produce numeri pseudorandom oppure un meccanismo ancora migliore. I numeri pseudocasuali danno cifrari sempre piuttosto sicuri, ma potenzialmente esposti a un attacco sufficientemente aggressivo.

In un vero one-time pad la chiave è lunga quanto il testo da cifrare. È la forza del sistema e, contemporaneamente, la sua debolezza, perché da una parte fornisce una sicurezza perfetta ma dall'altra parte lo scambio della chiave tra mittente e destinatario è critico. Un altro requisito è che nessuna parte della chiave venga mai riutilizzata per una cifratura successiva ed è questo il motivo per cui si chiama one-time, usa-e-getta.

Il metodo di cifratura in sé è molto semplice. Abbiamo il testo in chiaro (tic) e una chiave (key) che, applicata al testo, produrrà testo cifrato (cif). L'operazione è banale: un XOR bit per bit di chiave e testo in chiaro. Si può descrivere l'operazione anche così:

```
cif = key^tic
```

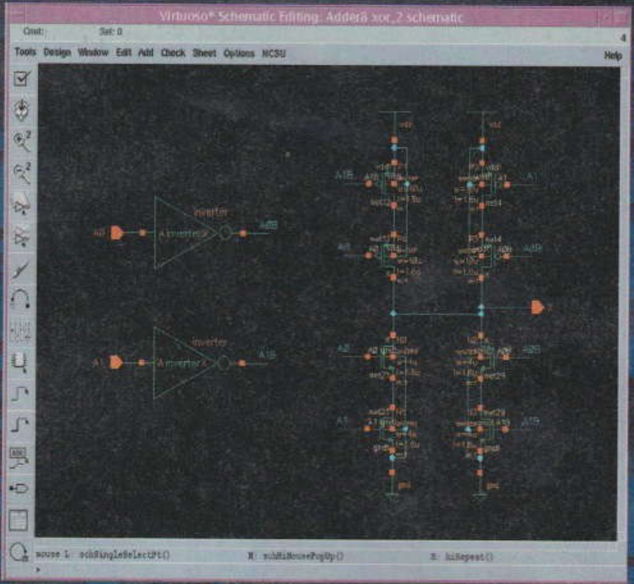
Per decifrare invece si fa:

```
tic = key^cif
```

SI FA PRESTO A DIRE RANDOM

I generatori di numeri casuali contenuti nei linguaggi di programmazione sono tutti pseudocasuali, ossia generano serie numeriche che prima o poi finiscono per ripetersi in qualche modo. Per generare numeri veramente casuali bisogna fare interagire l'algoritmo di calcolo con un evento naturale certamente casuale, come il decadimento di elementi radioattivi. La stessa definizione di numero casuale è in qualche modo problematica, anche se – molto rozzamente – si può dire che un numero è casuale quando è impossibile esprimere il numero usando meno bit di quanti ne contiene il numero. Sempre molto rozzamente, se un numero è veramente casuale, è impossibile comprimerlo. Un meccanismo molto semplice per generare numeri random è ricorrere a http://www.random.org, che parte dal rumore di fondo presente nell'atmosfera per ottenere numeri perfettamente casuali.

la chiave perfetta



È sorprendente come questo sia vero anche con messaggi e chiavi molto piccole. Supponiamo di essere gli aggressori e di intercettare un messaggio cifrato lungo, esageriamo, otto bit. Nella finzione, sappiamo che è una comunicazione tra terroristi e che se il messaggio consiste in una S ci sarà un attentato a una stazione, mentre se è una A è a rischio un aeroporto. Abbiamo già molte informazioni e tutto quello che ci manca è una piccola stupida chiave lunga otto bit, che può variare al massimo in 256 modi. Analizzandoli tutti, troveremo una chiave che genera una A e un'altra chiave che genera una S. Siccome tutte e due le chiavi sono ugualmente probabili, siamo al punto di partenza. Questo vale per messaggi di qualunque lunghezza.

La semplicità è davvero notevole. Ma se la chiave è veramente casuale, non viene scoperta ed è lunga quanto il messaggio, il cifrario è inviolabile. Infatti, se vengono rispettate le clausole che abbiamo specificato, un aggressore privo della chiave non può fare niente, neanche esaminare a forza bruta tutto lo spazio delle chiavi possibili. Provare tutte le chiavi teoricamente esistenti non porterà a nulla, in quanto un cifrario potrebbe dare con la stessa probabilità qualsiasi testo in chiaro.

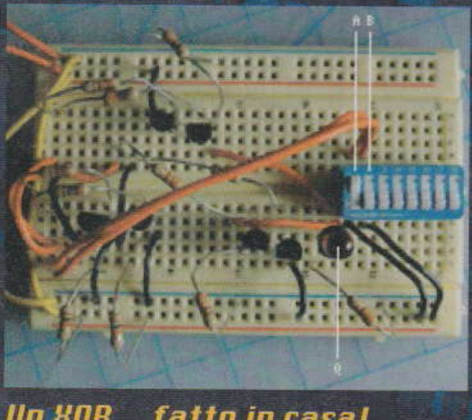
Certo, se un nostro agente riesce a scoprire la chiave tutto diventa più facile. Ed è per questo che i cifrari one-time pad non sono diventati l'unico sistema di cifratura usato al mondo.

XOR, L'OR ESCLUSIVO

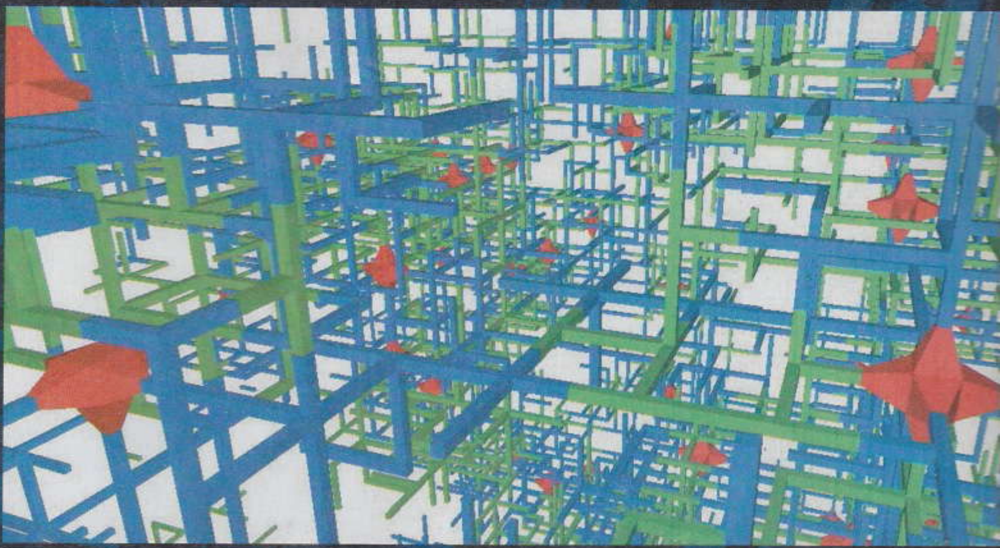
XOR è una delle operazioni tipiche dell'algebra booleana, riprodotte in tutte le salse dai gate elettronici di qualunque apparecchio digitale in commercio. In un gate (cancello) arrivano due segnali, ognuno dei quali può avere il valore di 0 oppure 1, e il gate lascia passare un singolo risultato che dipende da come sono accoppiati i due input. Il funzionamento di un gate viene tipicamente illustrato in schemini detti tabelle della verità, o truth table. Ecco la tabella della verità per XOR:

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

Kurt Gödel
kurtgoedel@hackerjournal.it



Un XOR... fatto in casa!



LADRI di



◄ *Una parte delicata del processo: la gelatina, colata sullo stampo ottenuto a partire dalla fotografia dell'impronta, è stata lasciata in frigorifero a rapprendere. Quando è sufficientemente fredda la si può distaccare con cautela dallo stampo.*

Ancora persuasi che la biometrica sia la risposta ai problemi della privacy? Beh, c'è gente che da una impronta digitale lasciata per strada fabbrica un dito sintetico a costo irrisorio. In Hacker Journal numero 51 avevamo mostrato come ricercatori giapponesi siano riusciti a produrre dita artificiali in grado di ingannare i sensori biometrici di impronte digitali al costo di un po' gelatina da cucina e poco altro.

I ricercatori avevano realizzato l'exploit partendo da dita vere di persone consenzienti, il fatto più eclatante – e inquietante – è che, anche se questa di per sé è una minaccia alla sicurezza del sistema, si possono realizzare dita artificiali a prescindere dal consenso della persona. È più difficile, ma è possibile. Basta una buona impronta lasciata dovunque.

Circuiti fotosensibili e gelatina

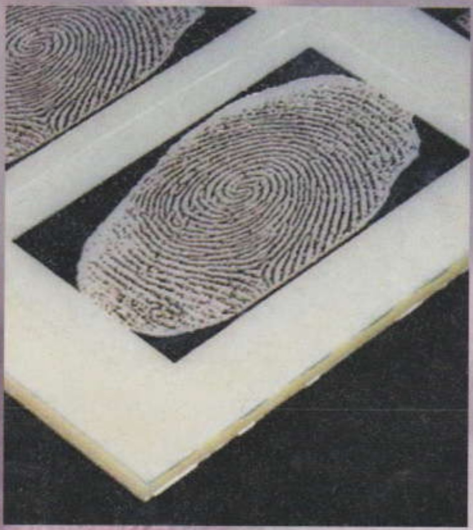
Sono un po' più complessi anche gli ingredienti. Alla consueta gelatina da cucina va aggiunta una scheda a circuiti stampati, sottile come un foglio di carta, ricoperta di uno strato fotosensibile, che reagisce alla luce.

L'impronta viene trattata come potrebbero fare gli agenti di CSI, il serial sulla polizia scientifica di Las Vegas: le tracce vengono evidenziate ricoprendole con adesivo cianoacrilico e fotografate ad alta risoluzione, se necessario con un microscopio elettronico, di cui esistono ormai esemplari altamente portatili. L'immagine risultante viene trattata con un programma di fotoritocco adeguato (da Photoshop in poi). Fino a qui è semplice: il problema è ottenere il rilievo, per arrivare all'impronta funzionante.

Dal modello allo stampo

L'immagine risultante dal lavoro di fotoritocco viene stampata con una buona inkjet (risoluzione tipo 1.200 x 600 dpi)

impronte



▲ Lo stampo pronto alla colata di gelatina. Si può arrivare a questo stadio a partire da una qualsiasi (buona) impronta lasciata per la strada!



◄ L'impronta finale ottenuta nella gelatina. Inganna molto facilmente qualunque sensore!



◄ L'impronta appena ottenuta dallo stampo. Fa impressione!

su pellicola trasparente. La stampa viene usata come una maschera e sovrapposta alla scheda a circuiti stampati fotosensibile. I due strati vengono sottoposti a raggi ultravioletti e, in pratica, si ottiene un negativo dell'impronta, perché la parte stampata della pellicola trasparente impedisce ai raggi UV di impressionare la zona fotosensibile sottostante.

La scheda impressionata viene lavorata per creare rilievi e avvallamenti corrispondenti alle tracce dell'impronta originale e arrivare così a uno stampo. Praticamente abbiamo una fotografia dell'impronta originale, con un leggero rilievo tridimensionale.

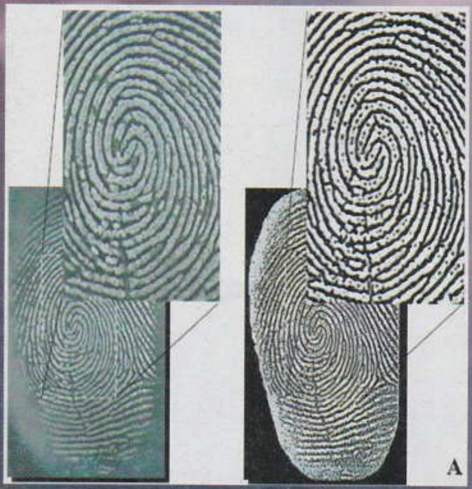
Conducente umido

È il momento della gelatina, che viene colata sopra l'impronta. Il tutto viene messo in frigorifero a raffreddare per una ventina di minuti, dopo di che si può staccare con delicatezza la gelatina rappresa, che riporta con fedeltà inquietante l'impronta originale.

Se l'operazione è stata condotta con cura (come farebbero aggressori sufficientemente motivati) e l'impronta di partenza è ragionevolmente buona, si possono ottenere impronte artificiali che arrivano a riprodurre non solo i tracciati, ma persino i pori della pelle, con caratteristiche di umidità e conducibilità che ricordano molto da vicino la pelle umana e sono nettamente superiori alle impronte realizzate in silicone.

Certo, ci vogliono tempo e lavoro. Ma tutto quello che abbiamo appena descritto è realizzabile in una casa qualsiasi, dotata di attrezzatura informatica normale e di una buona fotocamera digitale, abitata da una persona intraprendente con tempo da spendere.

Reed Wright
reedwright@mail.inet.it



▲ Dall'immagine fotografata dell'impronta all'immagine che servirà per produrre l'impronta è solo questione di Photoshop (o equivalente. Gimp è gratuito!).

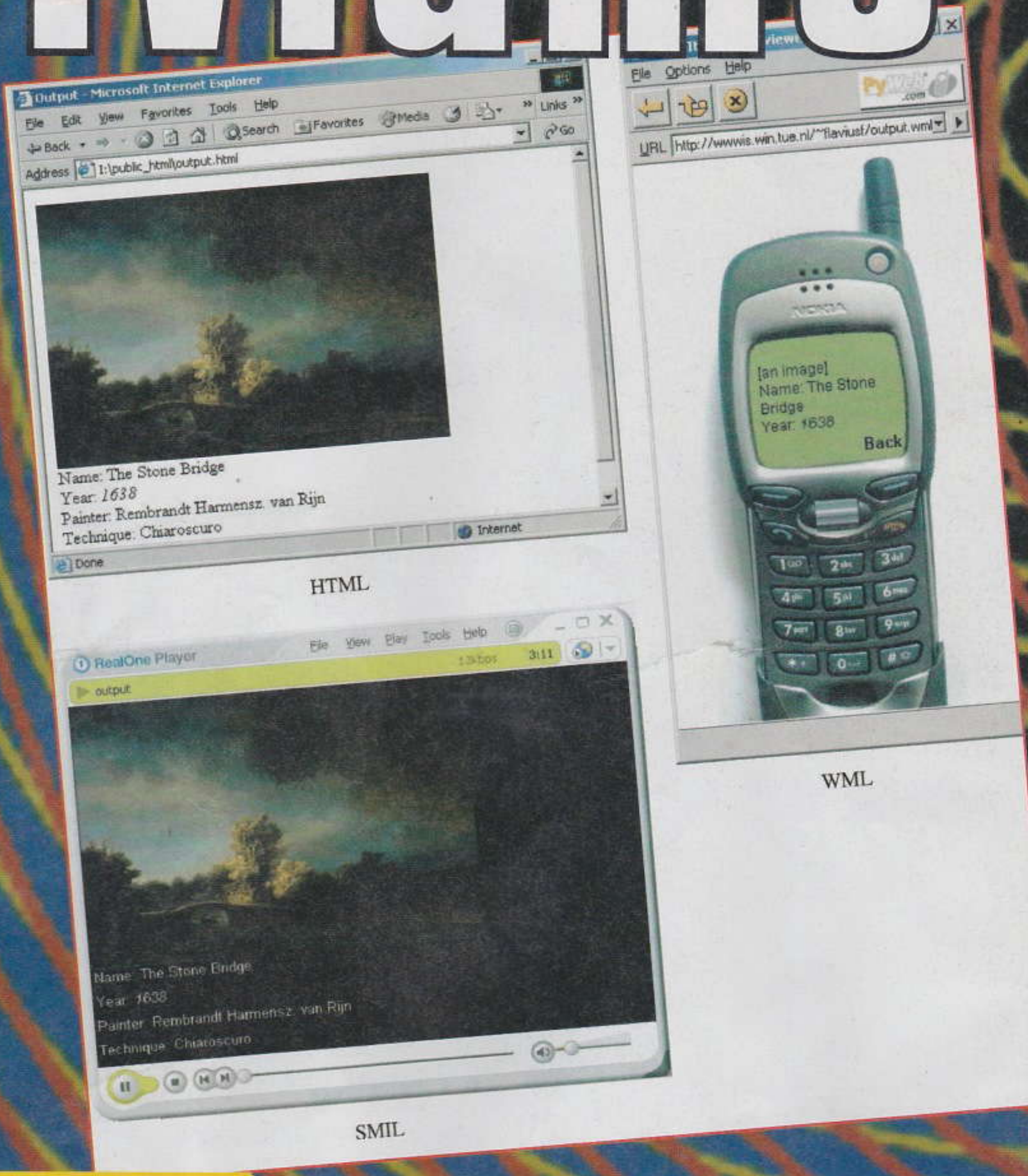
VIVO O DI GELATINA?

	Umidità	Conducibilità elettrica
Dito vero	16%	16 Mohm/cm
Dito di gelatina	23%	20 Mohm/cm
Dito di silicone	Non misurabile	Non misurabile

Le impronte digitali di gelatina ottenute con il metodo descritto da ricercatori giapponesi passano la prova dei sensori ottici e hanno un'alta probabilità di ingannare anche le apparecchiature più sofisticate, attente a umidità e conducibilità elettrica del "dito".

Scriviamo

Mettiamo servizi sempre nuovi a disposizione dei nostri cellulari



HTML

WML

SMIL

Solo pochi anni fa qualcuno diceva che nessuno avrebbe mai voluto guardare Internet dal minuscolo schermo di un cellulare. Basta guardare fuori dalla finestra per accorgersi che non è proprio vero.

WML (quasi) = HTML

Sappiamo tutti come nasce una pagina HTML. La si scrive, la si registra con suffisso .html e la si mette su un server che la rende visibile a tutti quelli che accendono un browser e si collegano a http://server/pagina.html, dove server è il la macchina su cui sta la pagina e pagina.html è il nostro file HTML.

il Linguaggio di marcatura wireless (Wireless Markup Language, WML) funziona con lo stesso principio, solo che è nato apposta per gli apparecchi con schermo piccolo, per esempio i cellulari. Una pagina WML si chiama card (scheda) e sta in deck (mazzi) e ha un suffisso .wml.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML
1.1//EN"
  "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
 <card id="Hello" title="Hello">
  <p>
   Hello from WML!
  </p>
 </card>
</wml>
```

◄ *Una semplice pagina scritta in WML.*

Dal server al browser

I server che ospitano WML devono essere capaci di farlo, ovvero sapere trattare i protocolli necessari. Tutti i server degni di questo nome, da Apache in giù, lo fanno più che degnamente, a patto di essere configurati a dovere.

Dato per scontato che un'occhiata alle

programmi WML

istruzioni, una telefonata al nostro provider o la dritta di un amico permetteranno di configurare un server in modo che possa presentare pagine WML, si pone il problema di come visionare le pagine preparate. Anche ammesso che il nostro browser standard sappia leggere il WML, di sicuro la sua finestra non equivale allo schermo di un cellulare. Serve quindi un browser WML.

Installato un browser qualsiasi, funziona come sul Web che conosciamo: digitiamo un indirizzo e vediamo la pagina. L'indirizzo potrebbe essere, per esempio, http://localhost/Hello.wml, per una pagina che sta su un server installato sul nostro computer.



◄ *Un browser WML in funzione su una pagina fin troppo semplice.*

Tag, card, deck

Come abbiamo detto, le pagine WML si chiamano card. Le card possono contenere testi, immagini, link, campi testo e meccanismi di inserimento dati o di selezione di opzioni. Siccome WML si basa su XML, tutti i tag che vengono aperti devono venire chiusi. Non ci sono certe libertà che sull'HTML sono invece consentite.

Testi, tabelle, immagini

Il testo si visualizza dentro tag di paragrafo:

```
<p align="left" mode="nowrap"/>
```

WML prevede tag table, img e tr, analoghi a quelli di HTML, anche se meno potenti. Le possibilità di formattazione del testo si fermano a corsivi, grassetti, enfasi e tag <strong>.

Link

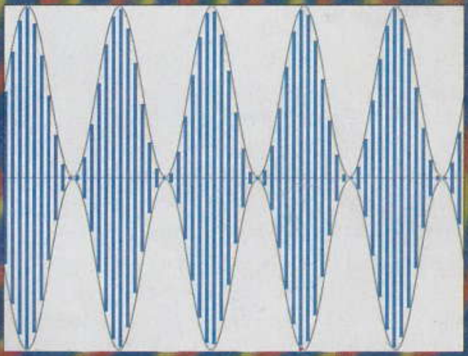
Per i link, WML mette a disposizione il tag a:

```
<a href="url" title="label" accesskey="1">testo o immagine linkata</a>
```

Label sta per il titolo del link, che va mantenuto entro i cinque caratteri di lunghezza per mantenere la compatibilità totale. accesskey mette un numero a sinistra del link, per consentire il "clic" premendo il numero appropriato sulla tastiera.

Verso l'input

Naturalmente queste sono solo le primissime basi del WML. Però dovrebbero bastare per consentire a tutti di scrivere una pagina WML anche estremamente elementare. Chi avesse voglia di inviare l'URL di una sua pagina WML visibile via cellulare scriva a guestbook@hackerjournal.it e sarà pubblicato. Prossimamente torneremo sull'argomento e affronteremo tematiche di WML più complesse, come le strutture di input dei dati e altro ancora.



▲ *Su onde come queste viaggiano le pagine WML lette dal nostro cellulare.*

BROWSER WML SUL WEB

Il browser Web migliore da cui partire è sicuramente WinWAP di Slob-Trot (http://www.slobtrot.com/eng/index.shtml). Vanno bene anche i browser di OpenWave, a http://www.openwave.com/us/products/mobile/device_products/.

Kurt Gödel
kurtgoedel@hackerjournal.it

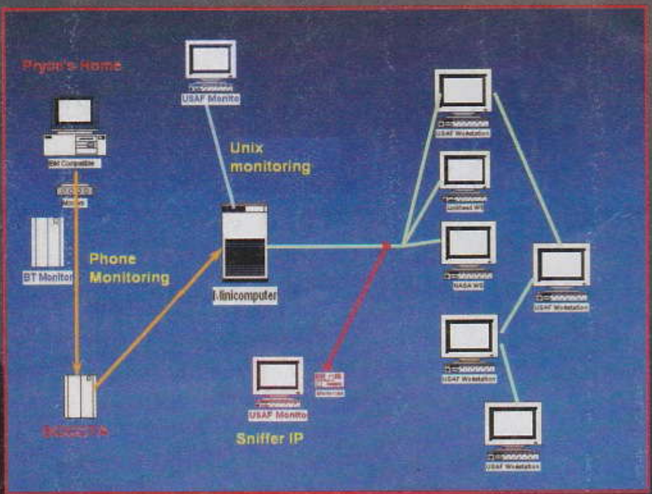
Troppo POCO spazio

Quando il maggiore Hinds dell'aeronautica militare degli Stati Uniti d'America accese il suo computer, la mattina del 28 marzo 1994, rimase a bocca aperta per almeno dieci secondi.



▲Le basi dell'Air Force negli Stati Uniti d'America. Datastream le ha bucate quasi tutte.

Nei successivi venti cercò con lo sguardo qualcuno intorno a sé. Dopodiché si disse che non era possibile e se qualcuno aveva voluto fargli uno scherzo l'avrebbe pagata cara.
Ma non era nello spirito, pur cameratesco, dei suoi colleghi di ufficio. Erano tutti addestrati a compiti estremamente specializzati di controllo elettronico e guerra informatica. Nella sua base, i Rome Labs della USA Airforce di stanza nello stato di New York, si studiavano sensori per la guerra elettronica. Gli occhi invisibili con cui vengono equipaggiati aerei spia e satelliti militari.
Eppure quel movimento non era stato rilevato da nessuno: dai log di sistema che gli apparivano ogni giorno sul video del suo pc, quella mattina risultava volatilizzata un'incredibile serie di file, tutti top secret e confidenziali, che erano stati trasferiti a un altro indirizzo IP, un computer esterno alla loro rete, chissadove. Doveva esserci un errore.
Dopo essersi attaccato al telefono per chiamare il generale Stevenson, a capo della baracca, si rilassò per un quarto d'ora. Il tempo per vedere arrivare, dalla sua finestra, le auto blindate dei "security experts and Computer Crime Investigators", che gli sembrarono tutti uguali, con quelle valigette nere e gli occhiali di protezione da un sole che ancora stentava, in quella mattina di primavera appena iniziata.



▲Per rintracciare Datastream l'esercito ha impiegato diversi sistemi di monitoraggio lungo tutte le linee utilizzate, a partire da quelle telefoniche.

Periferia di Londra, febbraio 1994

Il sedicenne Richard Pryce aveva assolto tutti i suoi compiti scolastici con grande sollievo dei genitori e si era appartato davanti al monitor del suo computer, come sempre. Non gli andava di guardare la TV e tantomeno di stare ad ascoltare i discorsi dei suoi, sulle pallose vicende che avevano reso la loro giornata tanto complicata.
Era da mesi, ormai, che aveva accumulato esperienza. Quasi per gioco, parlandone con gli amici, aveva scoperto le reti dati e i sistemi telefonici. Sapeva che telefonare a sbafo era una faccenda illecita, ma chi lo avrebbe mai scoperto? Si sentiva sicuro, coperto da quello che credeva l'anonimato dello schermo del suo pc. Il colpo migliore l'aveva messo a segno qualche mese prima. Sfruttando la debolezza di un servizio pubblico della compagnia telefonica di Bogotà, in Colombia, riusciva a farsi richiamare ogni volta che voleva a spese altrui e così poteva stare attaccato tutta la notte con il suo modem, senza spendere nemmeno una sterlina. A volte la linea era un po' disturbata, ma in compenso, immaginava, se avessero cercato di individuare la chiamata avrebbero iniziato dai sobborghi di Bogotà, non certo di Londra.

A capofitto dentro i server segreti

Si era fatto anche un amico più grande, Mathew Bevan, 21 anni appena compiuti, con cui riusciva a parlare a lungo, più che con tutti gli altri suoi compagni di clas-

sul DISCO



se. Avevano deciso assieme i nick da adottare in ogni comunicazione, tra loro e con altri. Lui decise per Datastream Cowboy, e Kuji il suo amico.
Dal provider di Bogotà, che ormai era diventato il loro trampolino per ripartire alla ricerca di indirizzi IP da esplorare, Kuji era riuscito a penetrare nel Goddard Space Center di un sistema a Latvia e a copiare i dati militari riguardanti tutta la zona Baltica. Dal canto suo, Datastream Cowboy era appena stato a fare una passeggiata (telematica, s'intende) nei sistemi della NATO a The Hague, nei Paesi Bassi, passando attraverso i server di Mindvox, un provider di New York.
Quando l'Air Force decise di monitorare le linee per sniffare i pacchetti IP e cercare di individuare l'intruso, Data stream Cowboy stava disconnettendosi dai server della base aerea Wright-Patterson in Ohio, usando come intermediario un sistema di Seattle: cyberspace.com.
Ma il panico nella base dell'Air Force si diffuse in aprile, quando Pryce penetrò in un sistema Koreano e trasferì il materiale del Korean Atomic Research Institute sui computer Air Force dei Rome Labs. La confusione isterica che ne seguì avrebbe potuto scatenare un vero incidente diplomatico, causato dall'aggressione telematica che poteva essere scambiata come un vero "atto di guerra".
Datastream Cowboy utilizzava un metodo molto semplice, ma altrettanto efficace. Piazzava su tutti i computer che trovava aperti sulla sua strada un keylogger, che gli forniva un'incredibile quantità di informazioni. Usare password, scoprire file top secret e divertirsi a trasferirli da remoto era ormai diventato un gioco da ragazzi.



▲Colindale, sobborgo di Londra. Scotland Yard individua in zona l'origine dei guai alle basi americane.



▲Bogota, Colombia. Da qui partivano le telefonate di Datastream per entrare nei sistemi segreti militari.

Il metodo e Scotland Yard

Cominciò a parlarne sui bulletin board, a cui cominciarono ad accedere anche gli agenti delle forze speciali. Con qualche semplice trucco di ingegneria sociale gli stessi riuscirono perfino a farsi dare il numero di telefono dall'intraprendente ragazzino. A fine aprile Scotland Yard ebbe così modo di ricevere istruzioni dall'intelligence americana di tracciare un certo numero di telefono dei sobborghi a nord est di Londra. Non ci misero nemmeno troppo a scoprire che il numero veniva utilizzato evitando di pagare le chiamate. Lo monitorarono per una decina di giorni e il 12 maggio intervennero. Quando si presentarono a casa di Pryce e questi capì che erano lì per arrestarlo, i testimoni raccontano che "si buttò per terra in posizione fetale e iniziò a piangere a dirotto".
Fu comunque un processo complicato e ricco di sorprese. I capi di imputazione erano tanti, ma solo con le investigazioni successive e l'analisi approfondita dell'hard disk di Datastream Cowboy, da cui vennero recuperati anche i dati di tracce cancellate, si ebbe conferma che era proprio lui il grande intruso. Il 21 giugno venne arrestato anche Kuji.
Durante gli interrogatori, Pryce confessò perfino di aver lasciato sul server del provider Mindvox il programma completo di intelligenza artificiale, appena creato dai laboratori dell'Air Force, per la simulazione delle guerre aeree. Perché? Troppo grande per essere trasferito sul suo hard disk, prima avrebbe dovuto buttare via qualcosa…

WriterBus

PROGRAMMAZIONE

Stop agli utenti non autorizzati



Come facciamo ad autenticare un utente che arriva sul nostro server Apache? Bastano pochi semplici mosse.

Usiamo Apache e il binomio PHP più MySQL. Ma non sarà il solito login da un form html: utilizzeremo gli header HTTP.
L'autenticazione degli utenti è infatti un problema da non sottovalutare ed è molto sentito da parte di tutti noi webmaster. Se creiamo delle aree di amministrazione o comunque nascoste agli utenti generici di Internet, capiamo subito l'esigenza di proteggerne l'accesso, magari indesiderato.
Per questo utilizziamo script o sfruttiamo le caratteristiche dei web-server (Apache in pool position), per custodire file e directory del proprio sito.

Il php

Anche il PHP interagisce al meglio con i web-server e può inviare al browser dell'utente degli header HTTP che richiedano nome utente e password.
Sfrutteremo questa caratteristica del PHP per la richiesta dei dati inseriti, che verranno poi cercati e paragonati con quelli presenti in una base dati MySQL.

Il database utenti

Dopo avere avviato MySQL (vedi box "EasyPHP 1.6, l'alternativa"), apriamo una sessione di DOS e dalla sottocartella \bin di MySQL lanciamo il client digitando mysql –u root.
Ora creiamo il DB utenti:

```
mysql> CREATE DATABASE utenti;
Query OK, 1 row affected (0.02 sec)
```

Oltre al testo da digitare (quello dopo la scritta 'mysql>'), abbiamo riportato anche la risposta da parte del server, mentre i comandi sono quelli in maiuscolo. Ricordiamoci sempre di terminare una riga di comando con il punto e virgola (;). Dopo aver creato il data base, utilizziamolo per inserirgli la tabella Lista_utenti:

```
mysql> USE utenti;
Database Changed

mysql> CREATE TABLE lista_utenti (
   -> id int(5) primary key not null
   auto_increment,
   -> nome varchar(50) not null,
   -> password varchar(50) not null,
   -> email varchar(100) not null,
   -> data varchar(20) not null,
   -> ip varchar(15) not null);
Query OK, 0 rows affected (0.01 sec)
```

Così vengono creati tutti i campi con le giuste dimensioni: per esempio 'id' sarà un numero intero con 5 cifre (fino a 99999) e gli altri campi di testo di lunghezze differenti.
Per le prove future, occorre che siano presenti dei dati all'interno del nostro DB. Ecco il codice per inserire un record, modificabile a piacimento:

```
mysql> INSERT INTO lista_utenti
VALUES
('','sonik','pluto','sonik@devpoint.it
','20/12/03 18:40','127.0.0.1');
Query OK, 1 row affected (0.00 sec)
```



▲ *I passaggi per accedere a \bin di MySQL e l'accesso a MySQL*

WEB





Ora che abbiamo preso un po' di confidenza con l'SQL, impariamo a visualizzare ciò che abbiamo appena inserito:

mysql> SELECT * FROM lista_utenti;					
id	nome	password	email	data	ip
1	sonik	pluto	sonik@devpoint.it	20/12/03 18:40	127.0.0.1
1 row in set (0.01 sec)					

L'output visualizzato viene automaticamente incasellato e così è anche bello da vedere!

Ora si comincia!

Abbiamo creato una base dati con un record valido e possiamo iniziare a scrivere il codice PHP. Cominciamo con la creazione del file [conn.php], relativo alla connessione e i suoi parametri.

```
<?
$data = date("d/m/Y H:i:s");
$server = "localhost";
$utente = "root";
$password = "";
$nome_db = "utenti";
$nome_tab = "lista_utenti";
```

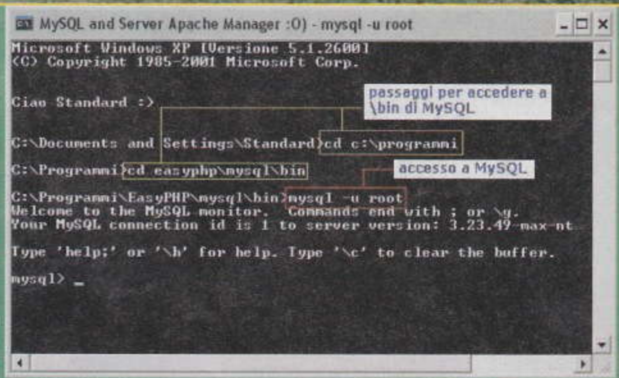
Questi sono tutte le variabili che utilizzeremo nel seguito del progetto, per non doverle ripetere e questo file sarà incluso in [index.php] che andremo a costruire. Ecco il resto:

```
$connessione = mysql_connect($server,$utente,$pass)
or die ("Non riesco a connettermi"); $db =
mysql_select_db($nome_db,$connessione) or die ("Non trovo il database");
```

Il file della root principale [index.php] avrà il compito di inviare gli header HTTP e, una volta che l'utente avrà avviato il login, di accertare che questi siano presenti nel DB.

Gli header

Sono in realtà di tipologie diverse e vanno inviati al browser prima di qualsiasi altra cosa, per evitare errori fastidiosi. Cominciamo con il creare il file [index.php].



▲ I passaggi per accedere a \bin di MySQL e l'accesso a MySQL

```
<?
if(!isset($PHP_AUTH_USER)) {
 header("WWW-Authenticate: Basic realm=\"Area Privata per admin\"");
 header("HTTP/1.0 401 Unauthorized");
 echo "Inserire nome utente e password per poter accedere";
 exit; }
```

Prima di proseguire, vediamolo a grandi linee. L'header "WWW-Authenticate" ci permette di definire l'area che presenta un accesso riservato (e il testo della label relativa). Il codice di stato HTTP 401 sta per "accesso negato" e lo si utilizza per monitorare quei casi in cui non sono stati inseriti username e password, oppure i dati digitati non sono corretti.

EASYPHP 1.6: L'ALTERNATIVA

Questo programma permette di avere nel proprio Windows, in un'unica installazione, il server Apache, MySQL e PHP avviabili insieme. Questo facilita la loro configurazione e permette il loro utilizzo anche a da parte di chi vuole provare l'alternativa Open Source al vecchio ASP su IIS (o PWS per Win9x).



Grazie a questo else ne controlliamo l'esistenza nella base di dati:

```
else {
  include('conn.php'); // la nostra connessione
```

La Query sul DB

Ora passiamo a creare la Query da eseguire sul DB:

```
$query = "SELECT id FROM $nome_tab WHERE nome = '$PHP_AUTH_USER' And password = '$PHP_AUTH_PW'";
```



http://localhost/HJ/ - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Avanti Termina Aggiorna

Indirizzo http://localhost/HJ/

AUTORIZZATO

nome utente: **sonik**
password : **pluto**

▲ Ok! Autorizzato!

```
$sql_query = mysql_query($query, $connessione) or die ("Non riesco a sviluppare la query");
```

In questo modo la Query può fornire un solo risultato o riga. Ecco come controllarne il valore:

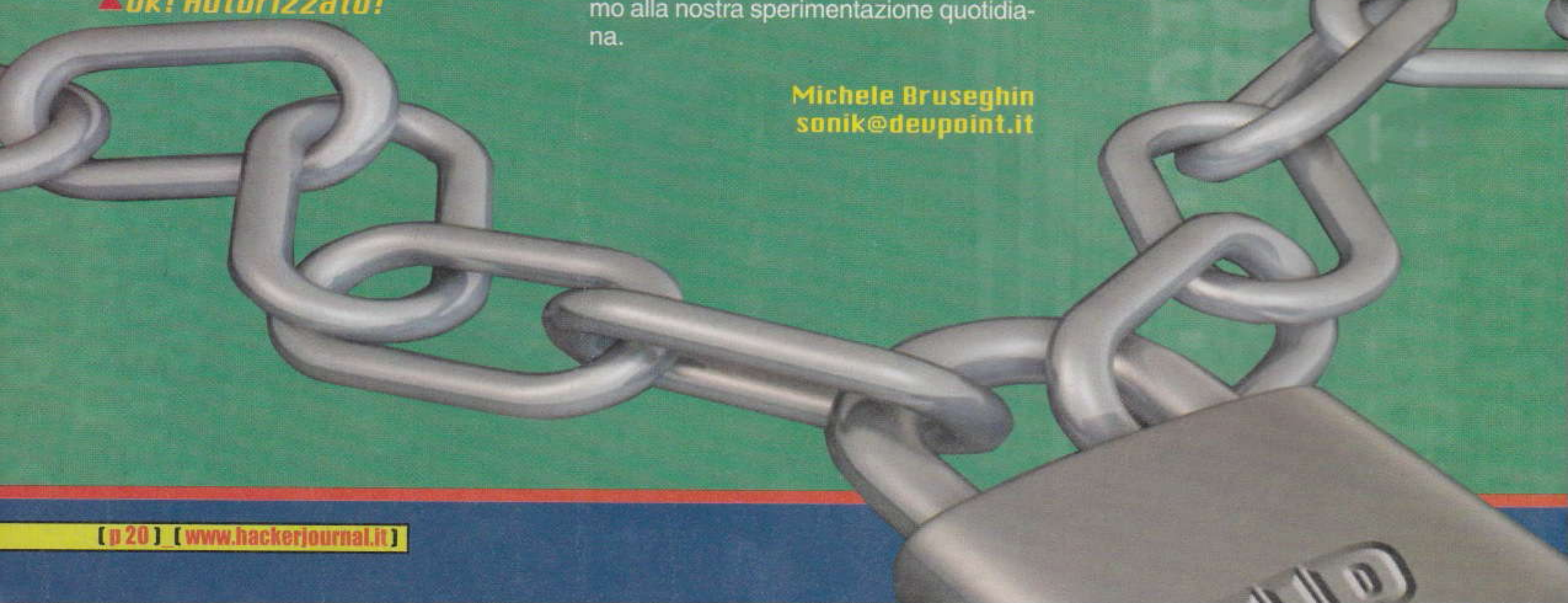
```
if($num_righe == '1') {
echo "<h1>AUTORIZZATO</h1>";
echo "<p>nome utente:
<b>$PHP_AUTH_USER</b><br />";
echo "password :
<b>$PHP_AUTH_PW</b></p>";
 }
```

Se otterremo un risultato che corrisponde a 1, il nome esiste e quindi la password corrisponde, altrimenti:

```
else if($num_righe == '0') {
echo "<h1>Nome utente e password non corretti</h1>";
echo "<a href='iscriviti.php'>iscriviti</a>";
 }
}
```

A questo punto bisognerebbe iscrivere l'utente nel database. Ma lo spazio è tiranno e invitiamo a scriverci per maggiori info sull'argomento. Per ora lo lasciamo alla nostra sperimentazione quotidiana.

Michele Bruseghin
sonik@devpoint.it



Un MOTORE di RICERCA in FLASH

Non solo animazioni un po' tutte uguali ma anche cose utili da usare, per esempio nelle pagine HTML incluse nei CD-Rom

Il compito è creare un motore di ricerca in Flash che si appoggi ad un file XML e che visualizzi fotografie a seconda di keyword cercate.

Servono:
- un file XML ;
- un Component, nella fattispecie il ListBox che si trova nella categoria Flash UI Components di Flash MX;
- un campo di testo Input;
- un campo di testo dinamico;
- un movie clip vuoto;
- un pulsante;
- un movie clip per contenere tutto quello descritto sopra.

Il file XML

Prima di tutto dobbiamo pianificare la struttura dei dati.

> **COSE DA TUTORIAL**
>
> Cose da sapere per affrontare questo tutorial:
> Conoscenza base di gestione e utilizzo di XML in Flash
> Conoscenza medio-alta di programmazione ActionScript
> Che cos'è e come si utilizza un array
> Come usare e programmare i Components

Per ora possono bastare tre campi per record:

cosatorna = Cosa dovrà essere visualizzato come risultato della ricerca
cosacarica = Cosa dovrà essere caricato dopo la scelta dell'utente
cosacerca = Quali dovranno essere le keyword di ricerca

Trattandosi di foto, un possibile file XML potrebbe essere:

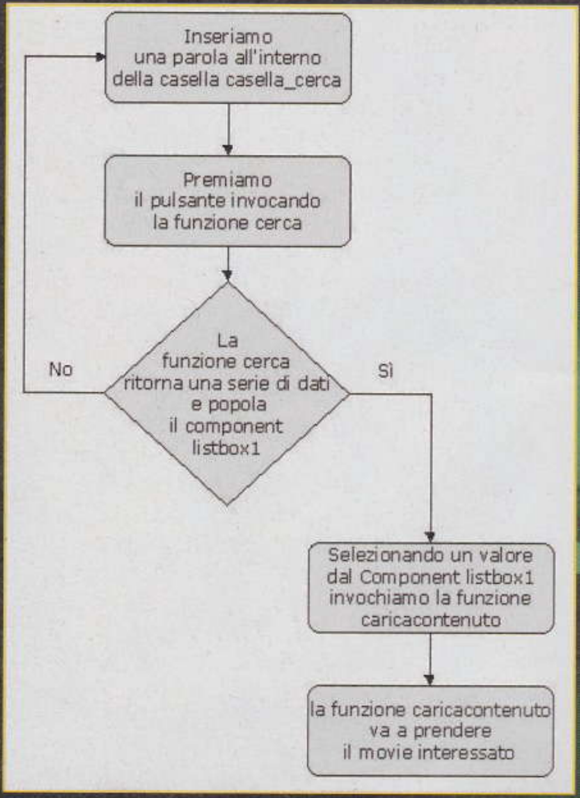
```
<motore>
<item cosatorna="Foto 1"
cosacarica="foto1.swf" cosacerca="paesaggio panorama tramonto
romantico"></item>
<item cosatorna="Foto 2" cosacarica="foto2.swf" cosacerca="paesaggio panorama alba
romantico"></item>
<item cosatorna="Foto 3" cosacarica="foto3.swf" cosacerca="paesaggio panorama mezzogiorno assolato"></item>
<item cosatorna="Foto 4" cosacarica="foto4.swf" cosacerca="paesaggio panorama mezzanotte silenzioso"></item>
</motore>
```

Ora realizziamo lo script ActionScript che dovrà leggere le informazioni:

```
onClipEvent (load) {
 Cosatorna = new Array();
 Cosacarica = new Array();
 Cosacerca = new Array();
 search_XML = new XML();
 search_XML.ignoreWhite = true;
 search_XML.onLoad =
function(evvai) {
 if (evvai) {
 parsailfile(search_XML);
 }
 };

search_XML.load("searchengine.xml
");
 function parsailfile(xmlDoc) {
 for (n=0; n<xmlDoc.firstChild.childNodes.length; n++) {
```





▲*Il diagramma di flusso del funzionamento del motore.*



```
Cosatorna.push(xmlDoc.firstChild.childNodes[n].attributes.cosatorna);

Cosacarica.push(xmlDoc.firstChild.childNodes[n].attributes.cosacarica);

Cosacerca.push(xmlDoc.firstChild.childNodes[n].attributes.cosacerca);
}
}
}
```

Il codice è all'interno di un onClipEvent (load), dato che tutto il motore starà in un movie clip.
Creiamo il movie clip, trasciniamolo sullo stage e inseriamo lo script.

Progettazione dell'interfaccia

Che cosa serve per creare l'interfaccia del motore di ricerca ?

- un posto per inserire le keyword: il campo di testo Input
- un pulsante per avviare la ricerca
- un Component per listare i risultati della ricerca: il ListBox
- un campo per un messaggio di errore nel caso non venga trovata nessuna occorrenza: il campo di testo dinamico

Apriamo quindi il nostro movie clip e d'ora in poi tutte le operazioni saranno effettuate al suo interno.

Il campo Input

Inseriamo sullo stage un campo di testo di tipo Input e nella casella dedicata al nome di variabile digitiamo casella_cerca.

Il campo dinamico

Inseriamo sullo stage un campo di testo di tipo dinamico e nella casella dedicata al nome di variabile digitiamo nofind.

Il pulsante di avvio

Inseriamo sullo stage un pulsante e digitiamo questo script nel pannello delle action:

```
on (release) {
 nofind = "";
 listbox1.removeAll();
 cerca();
 listbox1.sortItemsBy("label", "ASC");
 }
```

Il Component ListBox

Inseriamo sullo stage un Component di tipo ListBox, nominiamolo ListBox1 e digitiamo questo script nel pannello delle action:

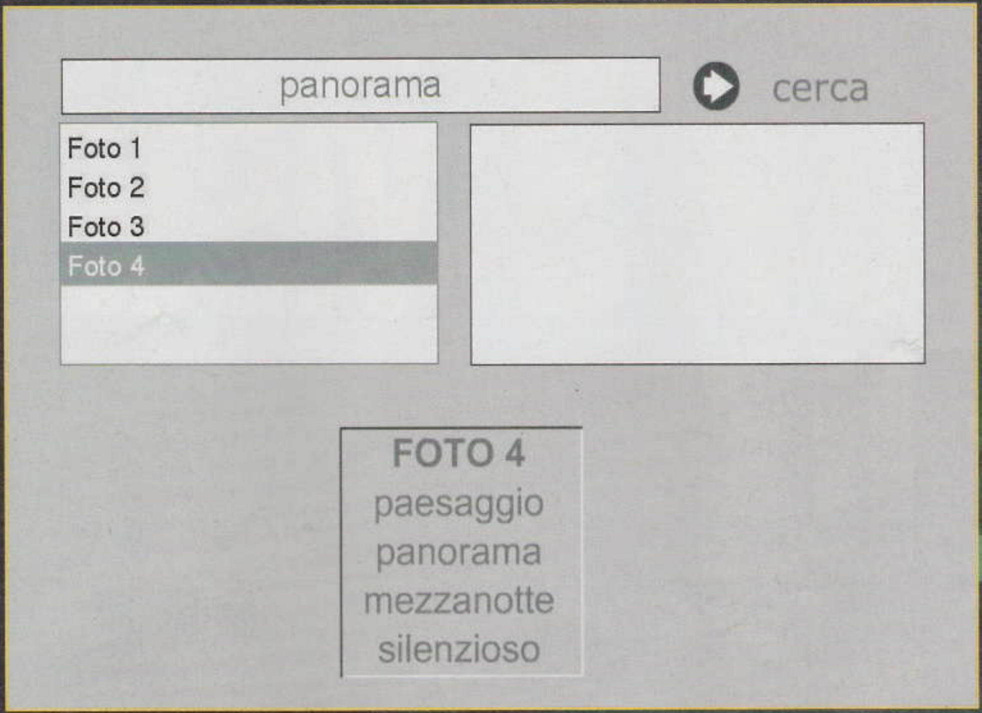
```
onClipEvent (load) { this.setAutoHideScrollBar(true);
}
 onClipEvent (enterFrame) {this.setChangeHandler("caricacontenuto");
 }
```

Lo script del motore

Eccoci allo script vero e proprio.
Nel primo frame della timeline del nostro movie clip inseriamo:

```
function caricacontenuto() {
 loadMovie(listbox1.getSelectedItem().data, MC_Ext);
 }

 function cerca() {
 for (a=0; a<Cosacerca.length; a++)
```



▲*Per una volta, ecco una cosa in Flash graficamente rudimentale ma di utilità pratica effettiva.*

IL MOTORE IN FUNZIONE

Si può vedere il motore di ricerca descritto in questo articolo all'indirizzo http://www.warp9.it/tutorial/flash/mx/searchengine/searchengine.swf.

```
{
 if (Cosacerca[a].toLowerCase().indexOf(casella_cerca.toLowerCase(), 1)
!= -1) {
 listbox1.addItem(Cosatorna[a],
Cosacarica[a]);
 }
 }
 if (listbox1.getLength() == 0) {
 nofind = "La ricerca non ha dato
nessun riscontro.";
 }
 }

 stop();
```

Qui definiamo le funzioni caricacontenuto e cerca.

La funzione cerca

```
for (a=0; a<Cosacerca.length; a++) {
```

Creiamo un ciclo for che andrà avanti tanto quanti saranno i valori dell'array Cosacerca.

```
(Cosacerca[a].toLowerCase().indexOf(casella_cerca.toLowerCase(),
1) != -1)
{
```

Riprendiamo la riga qui sopra. A parte toLowerCase() che serve per portare tutto in minuscolo evitando così problemi di ricerca, se il contenuto di casella_cerca applicato all'array Cosacerca è diverso (!=) da -1 allora si esegue:

```
listbox1.addItem(Cosatorna[a],
Cosacarica[a]);
```

cioè aggiungiamo nel Component listbox1 il contenuto dell'array Cosatorna per quanto riguarda label (la visualizzazione) e Cosacarica per quanto riguarda data (il dato da elaborare), altrimenti si passa oltre (ovvero non si fa niente).
Il ciclo si ripete un numero di volte uguale al numero dei valori contenuti nell'array Cosacerca.

Concludiamo la funzione con

```
if (listbox1.getLength() == 0) {
 nofind = "La ricerca non ha trovato
nessun riscontro, riprova con altre
chiavi.";
 }
```

La funzione caricacontenuto

Questa funzione verrà eseguita quando cliccheremo su uno dei valori del Component listbox1.
In questo esempio si è pensato di far caricare un movieclip esterno contenente la foto attraverso la tecnica ormai consolidata del movie clip vuoto, quindi creiamone uno, diamogli nome di istanza MC_Ext e trasciniamolo sullo stage.

```
loadMovie(listbox1.getSelectedItem().data, MC_Ext);
```

carica il movie esterno all'interno del movie clip vuoto con nome di istanza MC_Ext, prendendo il nome dalla selezione effettuata sul Component listbox1 con il valore memorizzato in data che, ricordiamo, è l'array Cosacarica.

Questo movie si può migliorare o arricchire in molti modi, l'importante è sperimentare.
Una base di partenza speriamo di averla fornita. :-)

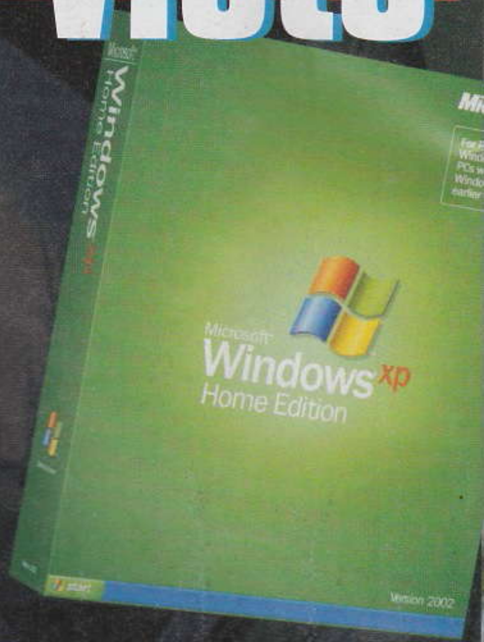
Warp9
http://www.warp9.it





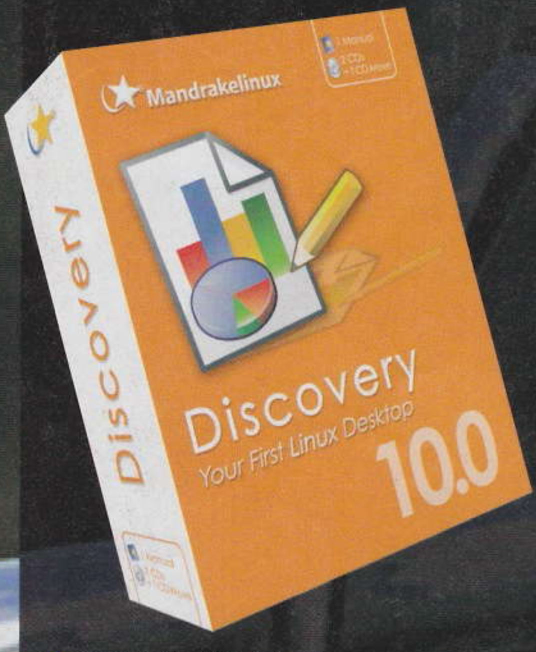
Windows visto da Linux

Un esperto di Linux si ritrova a tu per tu con Windows e non ne è contento. Vediamo se possiamo imparare qualcosa da lui



▲*Quanti programmi in questa scatola? Poco o niente. In una versione tipica di Linux ce ne sono decine.*

Sono passato a Linux prima che uscisse Windows XP. Non mi piaceva tanto quello che mi raccontavano del nuovo sistema e cercavo alternative.



▲*Mandrake Linux (http://www.mandrakelinux.com). Sarà semplice come suggerisce la confezione?*

Finalmente un amico mi ha consigliato Mandrake 8.1. Il resto, come si dice, è storia. I miei ultimi legami con Windows sono stati tagliati nel 2002, quando anche l'ultimo PC rimasto in casa è diventato un terminale Linux, e oggi la parte informatica della mia casa è Linux al cento per cento.

In questi due anni non mi era mai capitato di esaminare XP ed era diventato quasi una specie di gioco. Essere l'unica persona sulla Terra a non avere mai neanche visto XP, o qualcosa del genere. Poi ho risposto a una richiesta di aiuto che non potevo rifiutare e…

Lentooo...

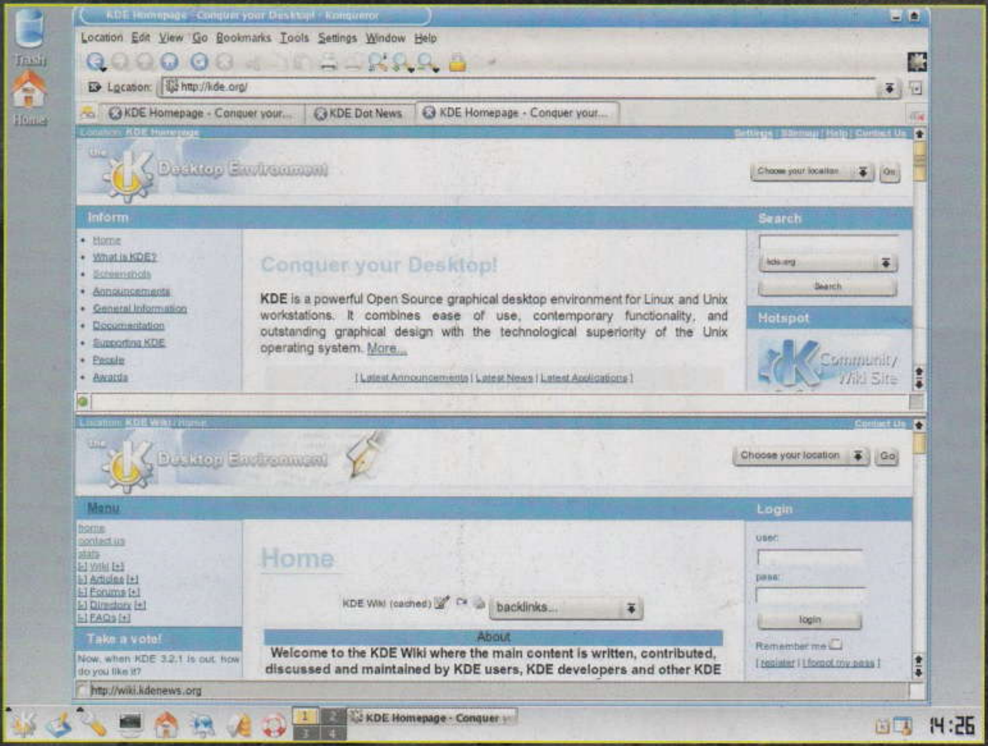
Mi sono ritrovato davanti a una macchina che andava terribilmente lenta. Non avevo idea del perché. Non potevo dare un comando top e scoprire che processo si portava via RAM o cicli di CPU. Ho tentato di usare il Task Manager, ma nessun processo mostrava segni di non rispondere e quindi non aveva senso impartire un comando kill per terminarlo.
Ho provato allora a vedere che tipo di hardware era montato sul computer. Ho armeggiato nelle Impostazioni, ma non sono riuscito a capire che CPU montasse, o quanta RAM ci fosse.

La persona che stavo cercando di aiutare era convinta che il computer fosse infettato da un virus, dato che lo scanner antivirus aveva riportato un problema con UNFILE.EXE. Il tentativo successivo fu di trovare e cancellare UNFILE.EXE, ma tutto andava troppo lentamente. Lo scanner sembrava non voler partire mai. Peraltro mi sembrava difficile che fosse colpa di un virus.

I messaggi di errore che uscivano, cercati su Google, non portavano a niente. Il modem ADSL era collegato ma se ne ricavavano solo timeout. Ho iniziato a fare ping in giro per vedere se c'era una connessione difettosa, un problema di DNS o altro. Niente. Nessun modo serio di vedere sotto il cofano quello che stava succedendo. Sembrava un Mac del secolo scorso, prima di Mac OS X.

Soccorso Linux

A un certo punto mi sono stufato e ho preso un CD di Knoppix, la versione di Linux



▲*KDE (http://www.kde.org), una delle interfacce grafiche più diffuse su Linux, ha un ottimo aspetto ed è assai funzionale.*

che funziona come fosse installata su un hard disk, senza dover toccare veramente i dati che sono sul computer. Un minuto ed ecco i dati della macchina: P4 a 2,4 GHz, 256 MB di RAM, video i845, audio i810, scheda di rete sis900 eccetera. Non c'era alcuna ragione per la lentezza che continuavo a constatare. Qualche cosa probabilmente mandava in confusione lo swap su disco.

Valutati i pro e i contro, si è deciso di formattare il disco. Ma prima, ancora un'ultima occhiata alla ricerca di qualche indizio utile. E mi sono reso conto che c'erano sei altri utenti amministratori installati. Li conoscevo: sei amici del liceo, tutti allegroni, nessun esperto. Nessuno di essi poteva avere idea di che cosa significa avere la responsabilità di essere root, e solo il cielo poteva sapere chi aveva combinato che cosa sul disco per avere quell'effetto. Spyware, adware, virus, worm, o altro, anche peggio. Meglio, davvero, formattare.

Ho impostato un account da amministratore e uno da utente, ripromettendomi di spiegare alla mia amica di usare l'account da utente per il lavoro quotidiano e usare l'account amministratore solo per i casi di emergenza. Nel mondo Linux questa cosa viene consigliata e spiegata da tutti; nel mondo Windows probabilmente non succede abbastanza.

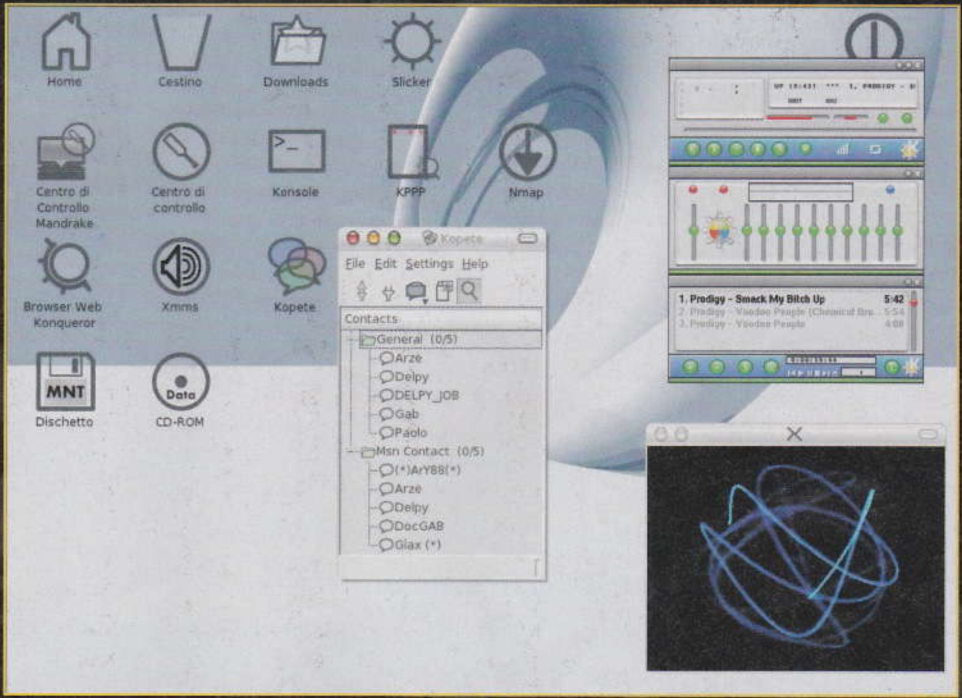
Nel frattempo l'installazione di Windows non riconosceva nessun componente hardware e per fortuna che sapevo che cosa era montato, altrimenti avrei passato ore a smanettare tra i driver. La mia Linux Debian due mesi fa mi aveva costretto a cercare una versione sperimentale di Xfree86 per fare andare la scheda video, ma XP voleva driver per ogni cosa.

Dove sono i programmi?

Alla fine XP si è installato. Una installazione Linux comprende decine, se non centinaia di programmi. E questa? Niente. Internet EXPloder, Outhouse EXPress e una interfaccia grafica più carina di quella di ME, ma sempre rudimentale. Mi sono stupito di quanto fosse lame l'interfaccia di XP rispetto a quella di KDE, perfino KDE 2.x.

Non so. Dicono che Linux sia più difficile di Windows. Certamente mia madre, che ha cinquant'anni e non sa quasi niente di computer, non sarebbe mai riuscita a installare Linux e ho dovuto farlo io per lei. Ma da allora non ha avuto più bisogno di niente.

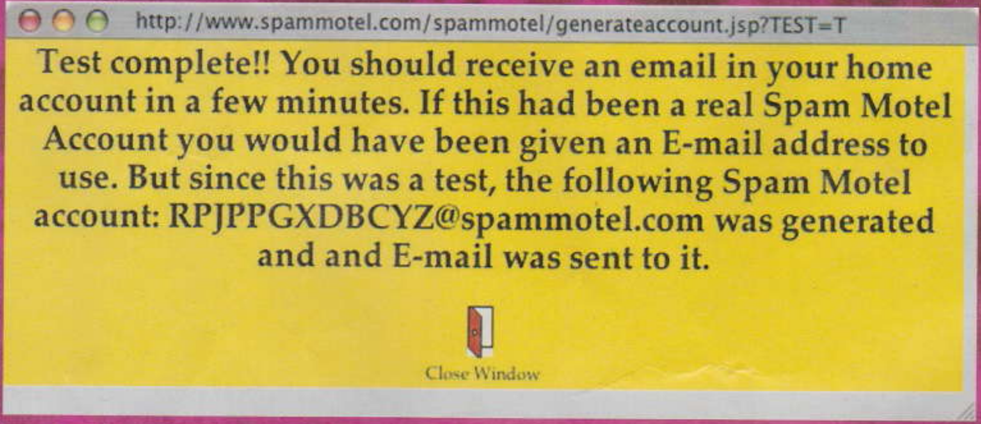
Silva



▲*Mandrake al lavoro. In italiano. Probabilmente anche nostra mamma potrebbe usarlo, se glielo installassimmo.*

Spam Motel
antispam innovativo

Spam Motel si raggiunge all'indirizzo prevedibile http://www.spammotel.com e, per quanto ancora in beta, sembra essere una buona soluzione nell'inseguimento continuo tra spammatori e soluzioni antispam.



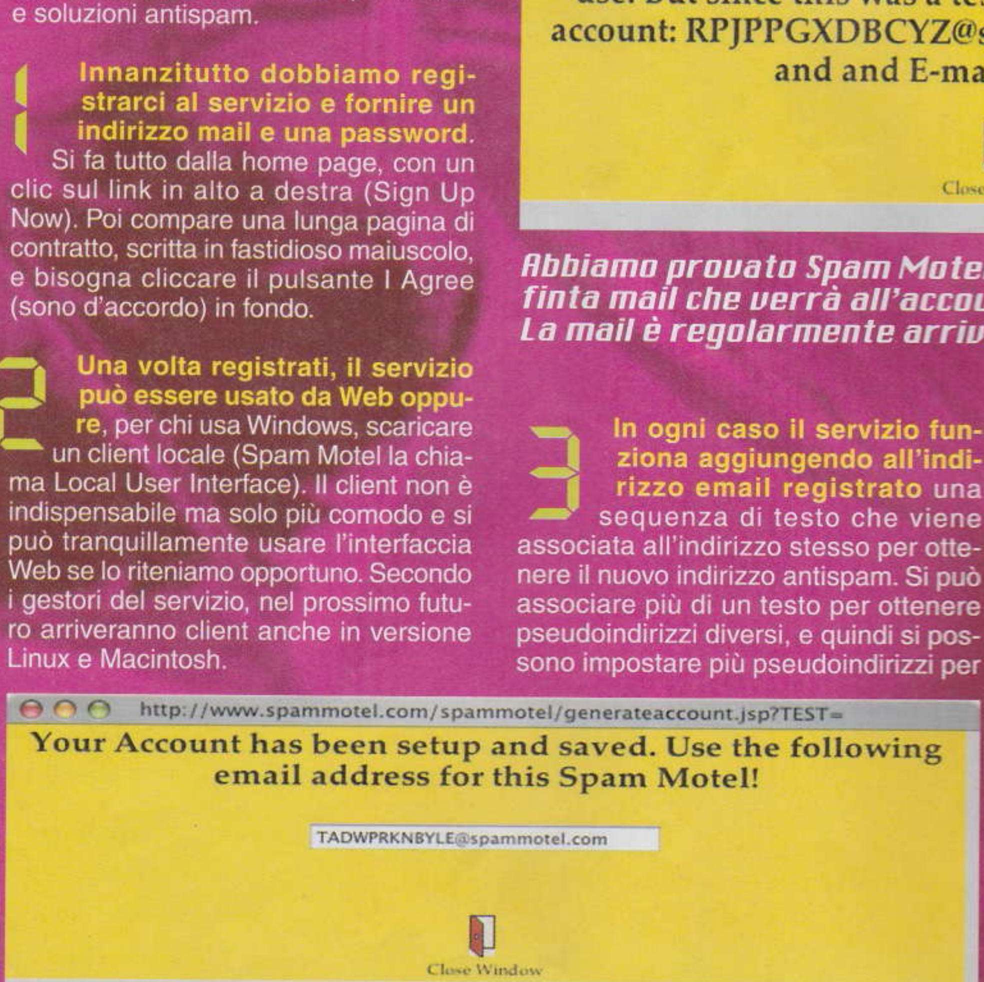
Abbiamo provato Spam Motel e il servizio ha generato una finta mail che verrà all'account con cui ci siamo registrati. La mail è regolarmente arrivata.

1 **Innanzitutto dobbiamo registrarci al servizio e fornire un indirizzo mail e una password**. Si fa tutto dalla home page, con un clic sul link in alto a destra (Sign Up Now). Poi compare una lunga pagina di contratto, scritta in fastidioso maiuscolo, e bisogna cliccare il pulsante I Agree (sono d'accordo) in fondo.

2 **Una volta registrati, il servizio può essere usato da Web oppure**, per chi usa Windows, scaricare un client locale (Spam Motel la chiama Local User Interface). Il client non è indispensabile ma solo più comodo e si può tranquillamente usare l'interfaccia Web se lo riteniamo opportuno. Secondo i gestori del servizio, nel prossimo futuro arriveranno client anche in versione Linux e Macintosh.

3 **In ogni caso il servizio funziona aggiungendo all'indirizzo email registrato** una sequenza di testo che viene associata all'indirizzo stesso per ottenere il nuovo indirizzo antispam. Si può associare più di un testo per ottenere pseudoindirizzi diversi, e quindi si possono impostare più pseudoindirizzi per ogni singolo indirizzo vero. Meglio scegliere testi descrittivi che aiutano a capire che uso ha ciascun indirizzo. Una volta finito si può provare l'efficacia del sistema con una mail di prova.

4 **Lavoriamo esattamente allo stesso modo per generare un account autentico.** Il messaggio di risposta del servizio è diverso ma la sostanza è identica: nasce un indirizzo che possiamo dare in giro senza rischio, almeno in teoria, di vederci inquinato dallo spam il nostro indirizzo autentico.



Ecco fatto: abbiamo pronto un nuovo indirizzo antispam, grazie a Spam Motel.

5 **Nelle opzioni possiamo impostare il ricevimento della posta in HTML**, cambiare l'indirizzo di forward delle mail-Spam Motel e l'eventuale inserimento di un testo di validazione a complicare ulteriormente la vita agli spammatori.

Sostituisce l'indirizzo email per ingannare i bot e gli altri pirati della posta elettronica



La sintonia fine degli pseudoindirizzi creati con Spam Motel.

6 **Una volta a regime, la gestione degli indirizzi è semplice e svelta.** Le attività principali sono la creazione di nuovi indirizzi quando serve, la modifica di quelli vecchi e il filtraggio o la sospensione di quelli troppo inquinati o sospetti. Gli indirizzi sospesi si possono riattivare a piacere.

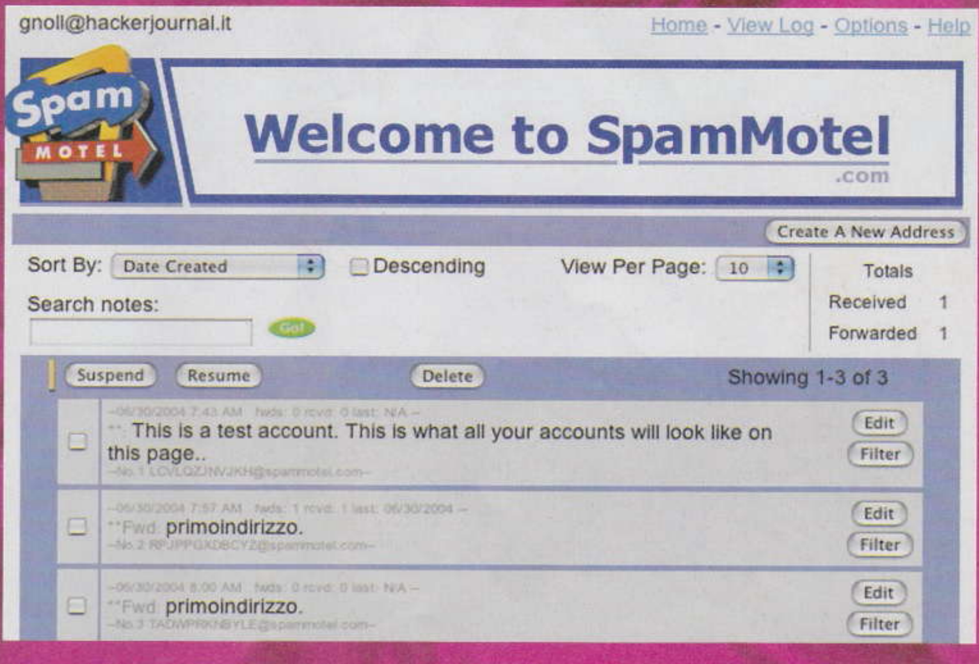
7 **Sarà veramente efficace nella lotta allo spam?**
Bella domanda. Il principio è ragionevolmente efficace: accettare che un account di posta possa essere compromesso e nel contempo disporre di un numero di account potenzialmente illimitato con cui rimpiazzare, diciamo, le vittime.

8 **Ci si può e deve chiedere quanto siano sicuri i meccanismi interni di Spam** Motel e se la gestione degli pseudoindirizzi non comporti per noi un problema di confidenzialità. Ma il servizio è giovane e a queste domande può rispondere con efficacia solo il tempo. Intanto Spam Motel esiste, offre un servizio interessante, non costa niente provarlo e, sinceramente, chi è afflitto dallo spam ed è in cerca di soluzione dovrebbe almeno prenderlo in considerazione.

I VANTAGGI DI SPAM MOTEL

Il succo dell'attività di Spam Motel è che possiamo vedere esattamente dove il mittente del messaggio che arriva ha recuperato il nostro indirizzo e indirettamente a chi lo ha passato, o venduto. I messaggi in arrivo da quel mittente possono essere bloccati con un clic del mouse.
Non esistono problemi di compatibilità; il sistema funziona, o promette di farlo, con qualsiasi programma su qualsiasi sistema. Anche sui computer diversi da Windows, per i quali manca attualmente il client locale, si può usare con pieno profitto l'interfaccia Web.

Barg the Gnoll
gnoll@hackerjournal.it



Una tipica schermata di gestione di Spam Motel. tutto molto facile e funzionale.

Come fa a mantenere la giusta qualità lo standard che fa girare la voce su Internet

VOCI che GIRANO



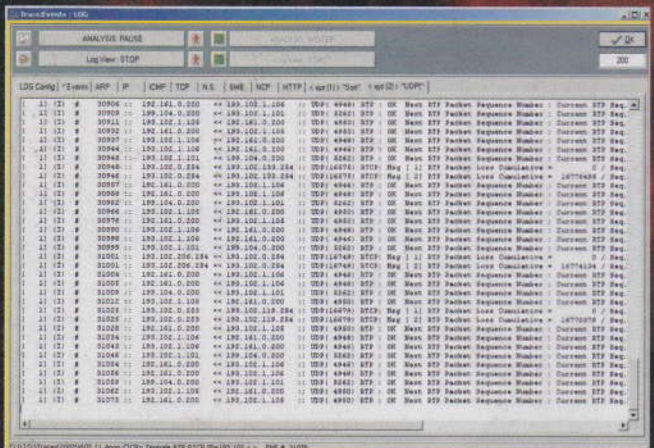
Abbiamo parlato qualche numero fa delle basi del protocollo VoIP, quello con cui possiamo fare chat audio e telefonare via IP. Adesso passiamo a nozioni più avanzate, per esempio come fa VoIP a mantenere la qualità della voce trasmessa sulla Rete.

Il protocollo RSVP

RSVP è un protocollo di segnalazione che si occupa di gestire, e se possibile mantenere, la cosiddetta Quality of Service (QoS). Richiede una certa quantità di banda e un certo valore di latenza in ciascun nodo di rete che lo supporta, valori indispensabili per consentire il passaggio della voce.

Qualità del servizio

La struttura di Internet è la cosa migliore possibile per i dati, ma la peggiore in assoluto per la voce in tempo reale. Su Internet infatti i dati viaggiano suddivisi in pacchetti. Ogni pacchetto segue la strada in quel momento migliore e, poiché la strada migliore cambia in continuazione, non è detto che i pacchetti arrivino nello stesso ordine in cui sono stati inviati, né che ci mettano lo stesso tempo. Se trasmettiamo il testo di questo articolo la cosa è irrilevante, ma se lo recitiamo in un microfono per un pubblico che ascolta è un disastro. I pacchetti di voce infatti devono



▲*L'incubo peggiore del VoIP: la perdita di pacchetti. Le voci si smozzicano e non si capisce più niente.*

MERITA UN LIBRO

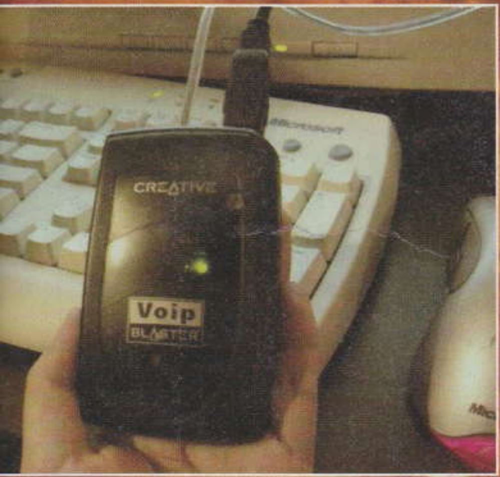
Il tema della Quality of Service merita un libro, non un articolo. Per studiarselo bene la prima cosa da fare è tuffarsi nella lettura dei Differentiated Services, seguendo i link che si trovano a http://www.ietf.org/html.charters/diffserv-charter.html e che puntano alle RFC 2474, 2475, 2597, 2893, 3086, 3140, 3246, 3247, 3248, 3260, 3289, 3290. Per raggiungere una IETF rapidamente, il link migliore è http://www.ietf.org/rfc/rfc3290.txt, sostituendo nell'ultima parte il numero della RFC cercata.



▲*Molte aziende sono passate da tempo, almeno internamente, alla telefonia IP per risparmiare. Lo sviluppo della telefonia IP sarà molto interessante nei prossimi anni.*

VoIP





PROTOCOLLO DI CORTESIA

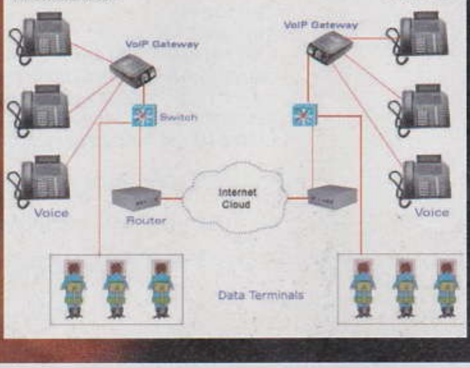
RSVP prende il nome dall'acronimo della frase francese Répondez s'il vous plait, che significa rispondete per favore e si mette in fondo agli inviti per richiedere una conferma. Tutti gli estremi del protocollo della cortesia applicato a Internet e a VoIP si trovano nella RFC 2205 (http://www.ietf.org/rfc/rfc2205.txt?number=2205)

arrivare nella sequenza esatta e non si può attendere a lungo un pacchetto ritardatario, poiché il parlato continua a fluire e i saluti iniziali, per fare un esempio sciocco, non possono certo arrivare a metà conferenza. TCP/IP non può garantire quello che chiediamo e così è necessario che ogni router che attraversiamo contenga gli accorgimenti adeguati per consentire VoIP. Uno di questi è il campo TOS in IP, il valore del quale determina l'urgenza del pacchetto (valore basso, urgenza alta). Poi ci sono i metodi di accodamento dei pacchetti stessi. Il metodo FIFO (First In First Out) è un non-metodo: i pacchetti passano come arrivano. Più intelligente è WFQ (Weighted Fair Queuing), che analizza i pacchetti in arrivo e vede chi deve passare prima, per esempio alternando un pacchetto UDP a un pacchetto TCP e vietando ai pacchetti FTP di prendersi tutta la banda libera al momento.

Nel sistema CQ (Custom Queuing) sono gli utenti a decidere le priorità. Nel PQ (Priority Queuing), invece, il flusso è suddiviso in varie code (tipicamente quattro) ciascuna con il suo livello di priorità. Dopo avere esaurito la prima coda si passa alla seconda e così via. Il sistema di accodamento più sofisticato è detto CB-WFQ (Class-Based Weighted Fair Queuing) ed è un WFQ con l'aggiunta di classi, fino a 64, che hanno ognuna un valore di banda passante associato. Dopo campo TOS e accodamento dei pacchetti abbiamo anche la limitazione della sorgente dati a un valore fisso in download o upload e i metodi di Congestion Avoidance (anticongestione) quali RED (Random Early Detection).

Nelle prossime esplorazioni di VoIP, dopo avere esaminato le viscere dello standard, arriveremo a questioni interessanti, come gli standard di videoconferenza e i requisiti hardware da rispettare.

Nyarlathotep
nyarlathotep@hackerjournal.it

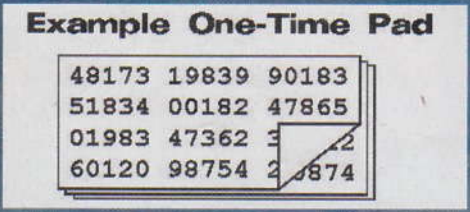




One-time pad

TANTE SOLUZIONI

Abbiamo giocato leggero all'inizio e pesante alla fine... ma sono arrivate risposte ottime!



GLI HACKER CHE HANNO RISPOSTO!

Il primo arrivato in assoluto è Simonide, super hacker! Ecco gli altri arrivati:

Na2SO4	Genio
Faicchio	Genio
SBRIK	Esperto
[2-p-a-c]	Esperto
-risolutore-	Genio
60LD3N R37R13V3R	Genio
pietrometal	Genio
The Alchemist	Genio
.:FireFox:.	Esperto
___NoWhereMan___	Genio
Paolo	Esperto
Federico Gorla	Esperto
C++	Esperto
.:..::Mauro il barelliere::..:.	Genio
Jett	Genio
..::Proz`HacK::..	Genio
Syther	Genio
dimmoniu	Esperto
Roby	SUPER HACKER
dark_devil	Genio
Devilangel666	Genio
Claudio	Esperto
~=[M37h0d]=~	SUPER HACKER
Fego	SUPER HACKER
Netrunner	Esperto
Enrico Sunseri	Genio
LordFly	Genio
LordDrago	Genio
Giuseppe De Roma	Genio
steno	Esperto
Vandryell	Genio
Black_cell	Esperto
Danykos	Esperto
Michele	Per tutti
dHo!	Per tutti
Ezio Rizzo	Genio
Dora Cammarota	Genio
AmatoHack86	Genio
sallatta	Genio

La soluzione

✪ **Per tutti:** se la chiave Anita dava come risultato DWEYEJOVIBMQRHFNO, la chiave Samantha avrebbe dovuto dare VJIFRCINHBYDWHMNT (qualcuno è riuscito a portare al cinema una sua amica Samantha? :-)

✪ **Per esperti:** la frase è **viva il software libero e abbasso ogni censura.**

✪✪ **Per geni:** esiste una sola chiave possibile ed è BIELOGPEIVEYQEGLDNDFDBOWEFZEFIVYSRQLBJ.

✪✪✪ **Per super hacker:** la frase è **hacker journal la rivista per tutti per esperti per geni e per super hacker.** Il sito http://www.vidwest.com/crypt/ permetteva di decifrare la risposta anche a chi non avesse saputo scrivere un programma apposta.

LA CIFRATURA JAVA DI DERBEER

```
import javax.swing.JOptionPane;
public class cripto
{
        public static void main (String []args)
        {
                JOptionPane.showMessageDialog(null,"Cripto Ver 1.0 by Derbeer");
                String f =JOptionPane.showInputDialog("Scrivi la frase senza spazi","Inserisci
la frase qui");
                String k = JOptionPane.showInputDialog(null,"Inserisci la chiave che vuoi
utilizzare");
                int ind =0;
                int ind2 =0;
                String alfa="abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz";
                char []alf= alfa.toCharArray(); //array alfabetico
                char []jk= new char[f.length()]; //array di appoggio
                char []c = k.toCharArray(); //array criptico
                char []t  =f.toCharArray(); //array frase

                        for (int q =0;q<f.length();q++) //riempie crittico
                        {
                                if (q<k.length()){
                                        jk[q]= c[q];
                                }else{

                                jk[q]=jk[(q-k.length())];
```

Marco Cariolato	Genio
One4Me	Genio
bauz	Genio
RiKi	Genio
.:marcuz:.	Genio
SIGMA5TH e YGUANEZ	Genio
<LEA>	Genio
AKIRA	Genio
retrogod aka zerokool	SUPER HACKER
Gabry89	Esperto
mK8	Genio
cyherbug	Esperto
yayo	Genio
Mario "Evildevil" Romano	Genio
!ToSsIc_ShAmRoCk88!	Genio
^MaNtRiX^	Esperto
Derbeer	Genio
Stefano	Genio
-=V3n0m=-	Genio
roy20021	Genio
Gabry89	Esperto
Marco	Genio
6Man6soN6	Genio

```
typedef unsigned char uns8;
typedef unsigned short uns16;

static uns8 state[256], x, y;    /* 256 octets of state information */

void
rc4init (key, length)     /* initialize for encryption / decryption */
    uns8 *key;
    uns16 length;
{
    int i;
    uns8 t;
    uns8 j;
    uns8 k = 0;

    for (i = 256; i--; )
       state[i] = i;

    for (i = 0, j = 0; i < 256; i++, j = (j + 1) % length)
        t = state[i], state[i] = state[k += key[j] + t], state[k] = t;

    x = 0;
    y = 0;
}

uns8
rc4step ()    /* return next pseudo-random octet */
{
   uns8 t;

   t = state[y += state[++x]], state[y] = state[x], state[x] = t;
   return (state[state[x] + state[y]]);
}
```

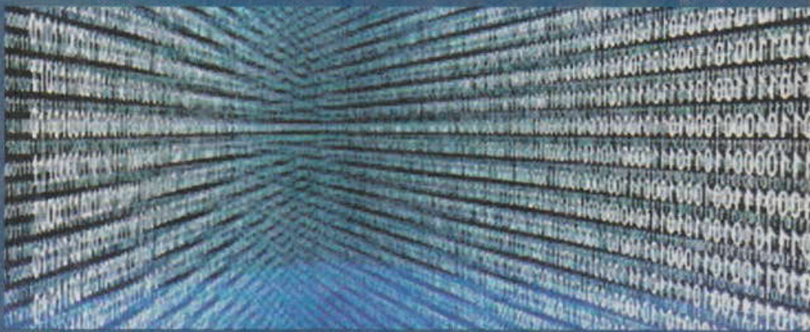


▲ *Anche Enigma, la macchina usata dai nazisti per cifrare nella seconda guerra mondiale, applicava una forma di cifrario one-time pad.*

RITARDATARI E DIVERSIVI

C'è sempre qualcuno che arriva dopo! O che aggiunge particolari.

Nagern sostiene che l'invocazione di soccorso aereo *Mayday* deriva dal francese M'aidez (aiutatemi) e lo stesso parere lo ha Bazze. In redazione Steso nota che in francese si dovrebbe dire Aidez moi, ma la questione resta aperta. Perché si dice Mayday?
RebelSource è riuscito a inviare i programmi VisualBasic per cifrare e decodificare gli aiuti di Avventura nel Castello. Lo stesso hanno fatto ThN1saHead e ftp21. CMOS ha invece decifrato le pergamene.
fox91 e tova hanno risposto Titanic, anno 1912 al Morse-problema.
frà Elia aveva mandato le stesse risposte in tempo, ma a un indirizzo sbagliato.
Complimenti a tutti comunque!



```
                    }
          }
//String a[]= new String[2];
for (int i = 0;i<f.length();i++){
          for (int j=0;j<26;j++)
          {
                    if (jk[i]==alf[j]) ind = j;
          }
          for (int j=0;j<26;j++)
          {
                    if (t[i]==alf[j]) ind2 = j;
          }
          //System.out.println("lettera "+t[i]+" numero: "+(ind+1)+"" );
          t[i]=alf[(ind+ind2)+1];
          ind =0;
          ind2 =0;
          //System.out.println(ind+1);
}
String w="";
for (int i =0;i<f.length();i++){
          //System.out.println(t[i]);
          w=w+t[i];
}
System.out.println("La frase criptata e': ");
System.out.println(w);
JOptionPane.showMessageDialog(null,"La frase criptata e': \n"+w);
System.exit(0);
     }
}
```

FACCIAMOCI TROVARE

Arrivano tante risposte. Per facilitarci il compito sarebbe meglio:

✍ scrivere nel subject Cyberenigma e il numero della rivista, meglio ancora il tema del cyberenigma;

✍ indicare chiaramente il nickname in fondo al messaggio;

✍ scrivere possibilmente prima che esca nuovamente HJ;

✍ se c'è un indirizzo di mail nella pagina del cyberenigma, usare quello e non altri.

Però facciamo comunque il possibile per tenere nota di tutti!

HACKER JOURNAL

IL PROSSIMO NUMERO IN EDICOLA IL 29 luglio 2004!

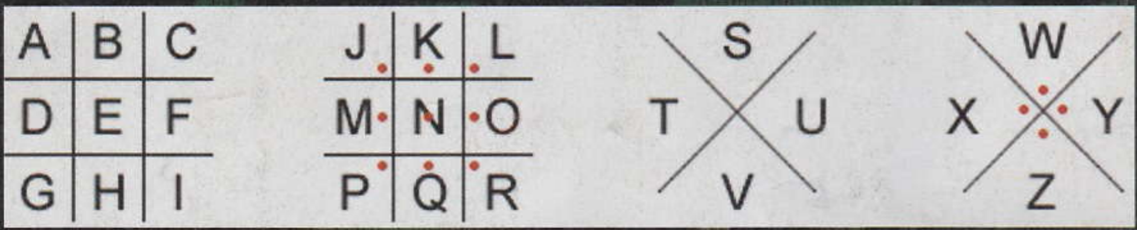
CYBERENIGMA



Un cifrario da fumetto!

Il cifrario di questo numero ha il nome identico a quello di un noto personaggio dei fumetti.

È un semplicissimo cifrario a sostituzione, che qualcuno di noi avrà usato alle scuole medie... o alle elementari! Si tratta di disporre le lettere dell'alfabeto intorno a quattro griglie.



Poi si scrive ogni lettera disegnando la parte di griglia che lo racchiude, con o senza puntino aggiunto.

a =

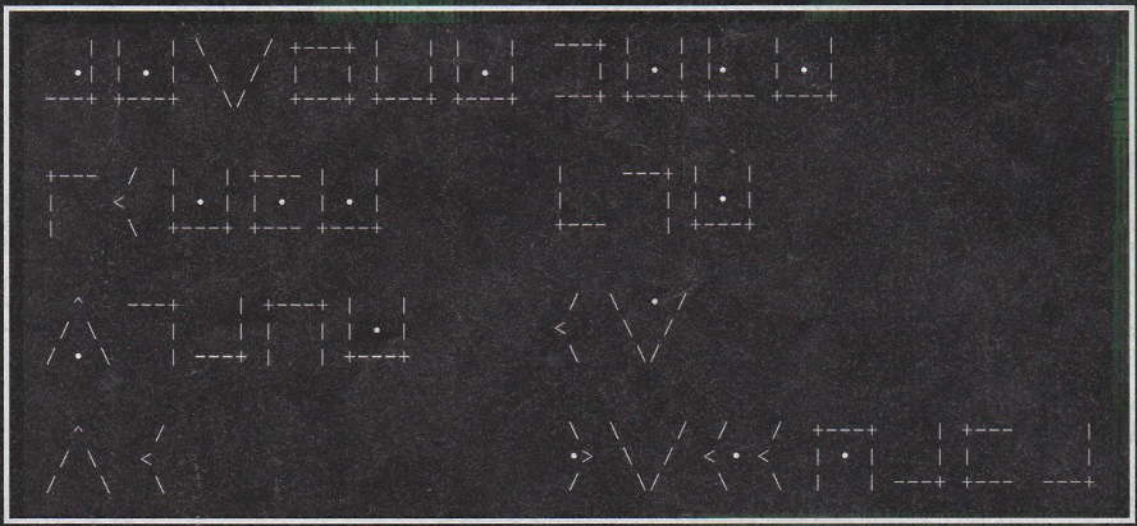
b =

c =

...

z =

Il messaggio segreto di questo numero è il seguente:



Solo che la corrispondenza tra lettere e simboli è stata cambiata!

L'aiutino: nel messaggio ci sono tutte le lettere dell'alfabeto italiano.

le risposte a:

guestbook@hackerjournal.it